VMware View-Installationshandbuch

View Manager 4.5
View Composer 2.5

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter http://www.vmware.com/de/support/pubs.

DE-000245-00

vmware®

Die neueste technische Dokumentation finden Sie auf der VMware-Website unter:

http://www.vmware.com/de/support/pubs/

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

Copyright © 2010 VMware, Inc. Alle Rechte vorbehalten. Dieses Produkt ist durch Urheberrechtsgesetze, internationale Verträge und mindestens eines der unter http://www.vmware.com/go/patents-de aufgeführten Patente geschützt.

VMware ist eine eingetragene Marke oder Marke der VMware, Inc. in den USA und/oder anderen Ländern. Alle anderen in diesem Dokument erwähnten Bezeichnungen und Namen sind unter Umständen markenrechtlich geschützt.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

Über dieses Handbuch 5

1 Systemanforderungen für Serverkomponenten 7
- View Connection Server-Anforderungen 7
- View Administrator-Anforderungen 9
- View Composer-Anforderungen 9
- View Transfer Server-Anforderungen 12

2 Systemanforderungen für Clientkomponenten 15
- Unterstützte Betriebssysteme für View Agent 15
- Unterstützte Betriebssysteme für View Client und View Client with Local Mode 16
- Hardwareanforderungen für Desktops im lokalen Modus 16
- Clientbrowseranforderungen für View Portal 18
- Unterstützung für Remote-Anzeigeprotokoll und -Software 18
- Adobe Flash-Anforderungen 22
- Anforderungen für die Smartcard-Authentifizierung 22

3 Vorbereiten von Active Directory 23
- Konfigurieren von Domänen und Vertrauensbeziehungen 23
- Erstellen einer OU für View-Desktops 24
- Erstellen von Organisationseinheiten und Gruppen für Clientkonten im Kiosk-Modus 24
- Erstellen von Gruppen für View-Benutzer 25
- Erstellen eines Benutzerkontos für vCenter Server 25
- Erstellen eines Benutzerkontos für View Composer 25
- Konfigurieren der Richtlinie „Restricted Groups (Eingeschränkte Gruppen)“ 26
- Verwenden von Gruppenrichtlinien-ADM-Vorlagendateien für View 26
- Vorbereiten von Active Directory für die Smartcard-Authentifizierung 27

4 Installieren von View Composer 31
- Vorbereiten einer View Composer-Datenbank 31
- Installieren des View Composer-Dienstes 38
- Konfigurieren der Infrastruktur für View Composer 39

5 Installieren von View Connection Server 41
- Installieren der View Connection Server-Software 41
- Konfigurieren von Benutzerkonten für vCenter Server und View Composer 56
- Anfängliches Konfigurieren von View Connection Server 60
- Konfigurieren von View Client-Verbindungen 64
- Größeneinstellungen für Windows Server zur Unterstützung Ihrer Bereitstellung 67

6 Installieren von View Transfer Server 75
Installieren von View Transfer Server 76
Hinzufügen von View Transfer Server zu View Manager 77
Konfigurieren des Transfer Server-Repositorys 78
Firewall-Regeln für View Transfer Server 80
Unbeaufsichtigte Installation von View Transfer Server 80

7 Konfigurieren der Zertifikatauthentifizierung 85
Ersetzen des Standardzertifikats 85
Hinzufügen von „keytool“ und „openssl“ zum Systempfad 86
Exportieren eines vorhandenen Microsoft IIS-SSL-Serverzertifikats 86
Erstellen eines neuen SSL-Zertifikats 87
Konfigurieren einer View Connection Server-Instanz oder eines Sicherheitsservers für die Verwendung eines neuen Zertifikats 91
Konfigurieren einer View Transfer Server-Instanz für die Verwendung eines neuen Zertifikats 92
Konfigurieren von SSL für Clientverbindungen 93
Konfigurieren von SSL für die View Transfer Server-Kommunikation 93
Verwenden von Gruppenrichtlinien zur Konfiguration der Zertifikatüberprüfung in View Client 94

8 Erstellen einer Ereignisdatenbank 95
Hinzufügen einer Datenbank und eines Datenbankbenutzers für View-Ereignisse 95
Vorbereiten einer SQL Server-Datenbank für die Ereignisberichterstellung 96
Konfigurieren der Ereignisdatenbank 97

9 Installieren und Ausführen von View Client 99
Installieren von View Client (Windows-basiert) oder View Client with Local Mode 99
Starten von View Client (Windows-basiert) oder View Client with Local Mode 101
Installieren von View Client unter Verwendung von View Portal 103
Installieren von View Client auf Mac OS X 104
Starten von View Client unter Mac OS X 105
Festlegen von Voreinstellungen für die virtuelle Druckfunktion 107
Verwenden von USB-Druckern 108
Unbeaufsichtigte Installation von View Client 108

Index 113

Über dieses Handbuch

Im *VMware View-Installationshandbuch* wird erläutert, wie Sie den VMware® View-Server und die Clientkomponenten installieren.

Zielgruppe

Dieses Buch ist für alle Benutzer gedacht, die VMware® View installieren möchten. Die Informationen in diesem Handbuch sind für erfahrene Windows- bzw. Linux-Systemadministratoren bestimmt, die mit der Technologie virtueller Maschinen und dem Betrieb von Rechenzentren vertraut sind.

VMware Technical Publications – Glossar

VMware Technical Publications stellt ein Glossar mit Begriffen bereit, mit denen Sie möglicherweise noch nicht vertraut sind. Definitionen für Begriffe, die in der technischen Dokumentation von VMware verwendet werden, finden Sie unter http://www.vmware.com/de/support/pubs (möglicherweise in englischer Sprache).

Feedback zu diesem Dokument

VMware freut sich über Ihre Vorschläge zum Verbessern der Dokumentation. Bitte senden Sie Ihre Kommentare und Vorschläge an docfeedback@vmware.com.

Technischer Support und Schulungsressourcen

Die folgenden technischen Supportressourcen stehen Ihnen zur Verfügung. Die neueste Version dieses Buchs und andere Bücher finden Sie unter http://www.vmware.com/de/support/pubs.

Online- und Telefonsupport

Um beim Online-Support technische Unterstützung anzufordern, Ihre Produkt- und Vertragsdaten abzurufen und Produkte zu registrieren, besuchen Sie http://www.vmware.com/de/support.

Kunden mit entsprechenden Supportverträgen erhalten über den Telefonsupport schnelle Hilfe bei Problemen der Prioritätsstufe 1. Besuchen Sie http://www.vmware.com/de/support/phone_support.html.

Supportangebote

Um herauszufinden, wie VMware mithilfe seines Supportangebots Ihre geschäftlichen Anforderungen erfüllen kann, besuchen Sie http://www.vmware.com/de/support/services.

VMware Professional Services

Die VMware Education Services-Kurse umfassen zahlreiche praktische Übungen, Fallbeispiele und Kursmaterialien, die bei der praktischen Arbeit als Referenz dienen. Die Kurse werden als Vor-Ort-Schulungen, Schulungen mit Kursleiter und als Online-Kurse bereitgestellt. Für Vor-Ort-Pilotprogramme und die Implementierung von empfohlenen Vorgehensweisen stellen die

VMware Consulting Services Angebote zur Bewertung, Planung, Erstellung und Verwaltung Ihrer virtuellen Umgebung bereit. Unter http://www.vmware.com/de/services finden Sie Informationen zu Schulungen, Zertifizierungsprogrammen und Beratungsservices.

Systemanforderungen für Serverkomponenten

1

Hosts, die VMware View-Serverkomponenten ausführen, müssen bestimmte Hardware- und Softwareanforderungen erfüllen.

Dieses Kapitel behandelt die folgenden Themen:

- „View Connection Server-Anforderungen“, auf Seite 7
- „View Administrator-Anforderungen“, auf Seite 9
- „View Composer-Anforderungen“, auf Seite 9
- „View Transfer Server-Anforderungen“, auf Seite 12

View Connection Server-Anforderungen

View Connection Server fungiert als Broker für Clientverbindungen, indem eingehende Anforderungen von Benutzern authentifiziert und an den entsprechenden View-Desktop weitergeleitet werden. Für View Connection Server gelten bestimmte Anforderungen in Bezug auf Hardware, Betriebssystem, Installation und unterstützende Software.

- Hardwareanforderungen für View Connection Server auf Seite 8

  Sie müssen View Connection Server auf einem dedizierten physischen oder virtuellen 32-Bit- oder 64-Bit-Computer ausführen, der bestimmte Hardwareanforderungen erfüllt.

- Unterstützte Betriebssysteme für View Connection Server auf Seite 8

  Sie müssen View Connection Server auf einem unterstützten Betriebssystem installieren.

- Anforderungen im Hinblick auf die Virtualisierungssoftware für View Connection Server auf Seite 8

  Für die ordnungsgemäße Funktion von View Connection Server müssen spezifische Anforderungen an die VMware-Virtualisierungssoftware erfüllt sein.

- Netzwerkanforderungen für replizierte View Connection Server-Instanzen auf Seite 9

  Wenn Sie replizierte View Connection Server-Instanzen installieren, konfigurieren Sie die Instanzen am selben Standort und verbinden Sie sie über ein Hochleistungs-LAN.

Hardwareanforderungen für View Connection Server

Sie müssen View Connection Server auf einem dedizierten physischen oder virtuellen 32-Bit- oder 64-Bit-Computer ausführen, der bestimmte Hardwareanforderungen erfüllt.

Tabelle 1-1. View Connection Server – Hardwareanforderungen

Hardwarekomponente	Erforderlich	Empfohlen
Prozessor	Pentium IV 2,0-GHz-Prozessor oder höher	Zwei Prozessoren
Netzwerk	Mindestens eine Netzwerkkarte mit 10/100 Mbit/s	Netzwerkkarten mit 1 Gbit/s
Arbeitsspeicher Windows Server 2008 64-Bit	4 GB RAM oder mehr	Mindestens 10 GB RAM für Bereitstellungen ab 50 View-Desktops
Arbeitsspeicher Windows Server 2003 32-Bit	2 GB RAM oder mehr	Mindestens 3 GB RAM für Bereitstellungen ab 50 View-Desktops

Diese Anforderungen gelten auch für zusätzliche View Connection Server-Instanzen, die Sie zum Erzielen von hoher Verfügbarkeit oder für den externen Zugriff installieren.

WICHTIG Der physische Computer bzw. die virtuelle Maschine, die View Connection Server hostet, muss eine statische IP-Adresse verwenden.

Unterstützte Betriebssysteme für View Connection Server

Sie müssen View Connection Server auf einem unterstützten Betriebssystem installieren.

In Tabelle 1-2 werden die für View Connection Server unterstützten Betriebssysteme aufgelistet.

Diese Betriebssysteme unterstützen alle Installationstypen von View Connection Server, einschließlich Standardserver-, Replikatsserver-, Sicherheitsserver- und View Transfer Server-Installationen.

Tabelle 1-2. Betriebssystemunterstützung für View Connection Server

Betriebssystem	Version	Edition	Service Pack
Windows Server 2008 R2	64 Bit	Standard Enterprise	–
Windows Server 2003 R2	32 Bit	Standard Enterprise	SP2
Windows Server 2003	32 Bit	Standard Enterprise	SP2

Anforderungen im Hinblick auf die Virtualisierungssoftware für View Connection Server

Für die ordnungsgemäße Funktion von View Connection Server müssen spezifische Anforderungen an die VMware-Virtualisierungssoftware erfüllt sein.

- Wenn Sie vSphere verwenden, müssen Sie über vSphere 4.0 Update 2 oder vSphere 4.1 verfügen.
- Wenn Sie VMware Infrastructure verwenden, müssen Sie über VMware Infrastructure 3.5 Update 5 und VirtualCenter Server 2.5 Update 6 verfügen.
- Sowohl ESX- als auch ESXi-Hosts werden unterstützt.

Netzwerkanforderungen für replizierte View Connection Server-Instanzen

Wenn Sie replizierte View Connection Server-Instanzen installieren, konfigurieren Sie die Instanzen am selben Standort und verbinden Sie sie über ein Hochleistungs-LAN.

Verwenden Sie kein Weitbereichsnetzwerk (Wide Area Network, WAN) zur Verbindung replizierter View Connection Server-Instanzen.

Selbst ein Hochleistungs-WAN mit niedriger Durchschnittslatenz und hohem Durchsatz erfüllt möglicherweise nicht immer die Leistungskriterien, die zur Erhaltung der Konsistenz zwischen den View Connection Server-Instanzen erforderlich sind.

Wenn die View LDAP-Konfigurationen auf View Connection Server-Instanzen inkonsistent werden, können Benutzer möglicherweise nicht auf ihre Desktops zugreifen. Einem Benutzer wird möglicherweise der Zugriff verweigert, wenn er oder sie eine Verbindung mit einer View Connection Server-Instanz herstellt, die eine veraltete Konfiguration verwendet.

View Administrator-Anforderungen

Administratoren verwenden View Administrator zum Konfigurieren von View Connection Server, Bereitstellen und Verwalten von Desktops, Steuern der Benutzerauthentifizierung, Initiieren und Untersuchen von Systemereignissen sowie Durchführen von Analysen. Clientsysteme müssen bestimmte Anforderungen erfüllen, um View Administrator auszuführen.

View Administrator ist eine webbasierte Anwendung, die zusammen mit View Connection Server installiert wird. Sie können für den Zugriff auf und die Verwendung von View Administrator die folgenden Webbrowser verwenden:

- Internet Explorer 7
- Internet Explorer 8
- Firefox 3.0
- Firefox 3.5

Zur Verwendung von View Administrator mit Ihrem Webbrowser müssen Sie Adobe Flash Player 10 installieren. Ihr Clientsystem muss Zugriff auf das Internet besitzen, damit Adobe Flash Player installiert werden kann.

Für eine ordnungsgemäße Textanzeige in View Administrator sind Microsoft-spezifische Schriftarten erforderlich. Wenn Ihr Webbrowser auf einem Nicht-Windows-Betriebssystem wie Linux, UNIX oder Mac OS ausgeführt wird, müssen Sie sicherstellen, dass Microsoft-spezifische Schriftarten auf Ihrem Computer installiert sind.

Derzeit werden auf der Microsoft-Website keine Microsoft-Schriftarten bereitgestellt, Sie können die Schriftarten jedoch von unabhängigen Websites herunterladen.

View Composer-Anforderungen

View Manager verwendet View Composer, um mehrere Linked-Clone-Desktops aus einem einzigen zentralen Basis-Image bereitzustellen. Für View Composer gelten bestimmte Installations- und Speicheranforderungen.

- Unterstützte Betriebssysteme für View Composer auf Seite 10

  View Composer unterstützt 64-Bit- und 32-Bit-Betriebssysteme mit spezifischen Anforderungen und Einschränkungen. Sie müssen View Composer auf demselben physischen Computer bzw. derselben virtuellen Maschine wie vCenter Server installieren.

- Datenbankanforderungen für View Composer auf Seite 10

  Für View Composer ist eine SQL-Datenbank zum Speichern von Daten erforderlich. Die View Composer-Datenbank muss sich auf dem vCenter Server-Computer befinden oder für diesen verfügbar sein.

- Anforderungen im Hinblick auf die Virtualisierungssoftware für View Composer-Funktionen auf Seite 11

  Sie müssen virtuelle Linked-Clone-Maschinen auf Hosts erstellen, die ESX/ESXi 4 oder höher ausführen, und Linked-Clone-Pools im vSphere-Modus konfigurieren, um den Vorteil verschiedener View Composer- und vSphere-Funktionen zu nutzen.

Unterstützte Betriebssysteme für View Composer

View Composer unterstützt 64-Bit- und 32-Bit-Betriebssysteme mit spezifischen Anforderungen und Einschränkungen. Sie müssen View Composer auf demselben physischen Computer bzw. derselben virtuellen Maschine wie vCenter Server installieren.

64-Bit-Betriebssysteme

Tabelle 1-3 listet die für View Composer unterstützten 64-Bit-Betriebssysteme auf.

Tabelle 1-3. 64-Bit-Betriebssystemunterstützung für View Composer

vCenter Server-Version	Betriebssystem	Service Pack	Edition
4.1	Windows Server 2008 R2	–	Enterprise
4.1	Windows Server 2008	SP2	Enterprise
4.1	Windows 2003 R2	SP2	Standard
4.1	Windows 2003	SP2	Standard
4.0 Update 2	Windows Server 2008	SP2	Enterprise

32-Bit-Betriebssysteme

Tabelle 1-4 listet die für View Composer unterstützten 32-Bit-Betriebssysteme auf.

Tabelle 1-4. 32-Bit-Betriebssystemunterstützung für View Composer

vCenter Server-Version	Betriebssystem	Service Pack	Edition
4.0 Update 2	Windows Server 2003	SP2	Standard
2.5 Update 6	Windows Server 2003 R2	SP2	Standard
2.5 Update 6	Windows Server 2003	SP2	Enterprise

Datenbankanforderungen für View Composer

Für View Composer ist eine SQL-Datenbank zum Speichern von Daten erforderlich. Die View Composer-Datenbank muss sich auf dem vCenter Server-Computer befinden oder für diesen verfügbar sein.

Wenn bereits ein Datenbankserver für vCenter Server vorhanden ist, kann View Composer diesen vorhandenen Datenbankserver nutzen, wenn es sich um eine in Tabelle 1-5 aufgeführte Version handelt. View Composer kann zum Beispiel die zusammen mit vCenter Server bereitgestellte Microsoft SQL Server 2005 Express-Instanz verwenden. Wenn noch kein Datenbankserver vorhanden ist, müssen Sie einen solchen installieren.

View Composer unterstützt eine Teilmenge der von vCenter Server unterstützten Datenbankserver. Wenn Sie vCenter Server bereits mit einem Datenbankserver verwenden, der nicht von View Composer unterstützt wird, verwenden Sie diesen Datenbankserver weiterhin für vCenter Server, und installieren Sie einen separaten Datenbankserver für View Composer- und View Manager-Datenbankereignisse.

WICHTIG Wenn Sie die View Composer-Datenbank auf derselben SQL Server-Instanz erstellen wie für vCenter Server, achten Sie darauf, nicht die vCenter Server-Datenbank zu überschreiben.

In Tabelle 1-5 werden die unterstützten Datenbankserver und -versionen aufgeführt. Eine vollständige Liste der von vCenter Server unterstützten Datenbankversionen finden Sie unter *VMware vSphere Compatibility Matrixes (VMware vSphere-Kompatibilitätstabellen)* auf der Dokumentationswebsite zu VMware vSphere.

Tabelle 1-5. Unterstützte Datenbankserver für View Composer

Datenbank	vCenter Server 4.1	vCenter Server 4.0 U2	VC Server 2.5 U6
Microsoft SQL Server 2000 SP4 Standard	Nein	Nein	Ja
Microsoft SQL Server 2005 Express	Ja	Ja	Ja
Microsoft SQL Server 2005 SP2 Standard und Enterprise	Ja	Ja	Ja
Microsoft SQL Server 2008 Standard und Enterprise	Ja	Ja	Nein
Microsoft SQL Server 2008 Standard und Enterprise, 64-Bit	Ja	Ja	Nein
Oracle 9i Release 2	Nein	Nein	Ja
Oracle 10g Release 2	Ja	Ja	Nein
Oracle 11g Release 1	Ja	Ja	Nein

Anforderungen im Hinblick auf die Virtualisierungssoftware für View Composer-Funktionen

Sie müssen virtuelle Linked-Clone-Maschinen auf Hosts erstellen, die ESX/ESXi 4 oder höher ausführen, und Linked-Clone-Pools im vSphere-Modus konfigurieren, um den Vorteil verschiedener View Composer- und vSphere-Funktionen zu nutzen.

- Speichern virtueller Linked-Clone-Maschinen in lokalen Datenspeichern
- Umleiten entbehrlicher Daten auf separate, nicht persistente Festplatten
- Speichern von Replikaten und verknüpften Klonen in separaten Datenspeichern
- Erstellen von Pools von einem Snapshot einer übergeordneten virtuellen Maschine, die Hardwareversion 7 verwendet
- Verwenden der Sysprep-Anpassungsspezifikationen für virtuelle Linked-Clone-Maschinen.

  Außerdem wird Sysprep nur unter vSphere 4.1-Software für verknüpfte Klone unterstützt. Sie können Sysprep nicht unter vSphere 4.0- oder VMware Infrastructure 3.5-Software verwenden.

View Transfer Server-Anforderungen

View Transfer Server ist eine optionale View Manager-Komponente, die das Einchecken, Auschecken und Replizieren von Desktops unterstützt, die im lokalen Modus ausgeführt werden. Für View Transfer Server gelten bestimmte Installations-, Betriebssystem- und Speicheranforderungen.

- Installationsanforderungen für View Transfer Server auf Seite 12

  Sie müssen View Transfer Server als Windows-Anwendung in einer virtuellen Maschine installieren, die bestimmte Anforderungen erfüllt.

- Unterstützte Betriebssysteme für View Transfer Server auf Seite 13

  Sie müssen View Transfer Server auf einem unterstützten Betriebssystem mit der erforderlichen Menge an Arbeitsspeicher (RAM) installieren.

- Speicheranforderungen für View Transfer Server auf Seite 13

  View Transfer Server überträgt statische Inhalte in das und aus dem Transfer Server-Repository sowie dynamische Inhalte zwischen lokalen Desktops und Remote-Desktops im Rechenzentrum. Für View Transfer Server gelten bestimmte Speicheranforderungen.

Installationsanforderungen für View Transfer Server

Sie müssen View Transfer Server als Windows-Anwendung in einer virtuellen Maschine installieren, die bestimmte Anforderungen erfüllt.

Die virtuelle Maschine, die View Transfer Server hostet, muss mehrere Anforderungen hinsichtlich der Netzwerkkonnektivität erfüllen:

- Die virtuelle Maschine muss von derselben vCenter Server-Instanz verwaltet werden wie die lokalen Desktops, die sie verwaltet.
- Die virtuelle Maschine muss nicht Teil einer Domäne sein.
- Die virtuelle Maschine muss eine statische IP-Adresse verwenden.

Vorsicht Sie müssen die virtuelle Maschine, die View Transfer Server hostet, mit einem LSI Logic Parallel-SCSI-Controller konfigurieren. Sie können keinen SAS- oder paravirtuellen VMware-Controller verwenden.

Auf virtuellen Windows Server 2008-Maschinen ist der LSI Logic-SAS-Controller standardmäßig ausgewählt. Sie müssen diese Auswahl vor Installation des Betriebssystems in einen BusLogic- oder LSI Logic-Controller ändern.

Die View Transfer Server-Software darf nicht auf derselben virtuellen Maschine wie eine andere View Manager-Softwarekomponente vorliegen, View Connection Server eingeschlossen.

Sie können zum Erzielen von hoher Verfügbarkeit und Skalierbarkeit mehrere View Transfer Server-Instanzen installieren.

Unterstützte Betriebssysteme für View Transfer Server

Sie müssen View Transfer Server auf einem unterstützten Betriebssystem mit der erforderlichen Menge an Arbeitsspeicher (RAM) installieren.

Tabelle 1-6. Betriebssystemunterstützung für View Transfer Server

Betriebssystem	Version	Edition	Service Pack	RAM-Mindestgröße
Windows Server 2008 R2	64 Bit	Standard Enterprise	–	4 GB
Windows Server 2003 R2	32 Bit	Standard Enterprise	SP2	2 GB
Windows Server 2003	32 Bit	Standard Enterprise	SP2	2 GB

WICHTIG Konfigurieren Sie zwei virtuelle CPUs für virtuelle Maschinen, die View Transfer Server hosten.

Speicheranforderungen für View Transfer Server

View Transfer Server überträgt statische Inhalte in das und aus dem Transfer Server-Repository sowie dynamische Inhalte zwischen lokalen Desktops und Remote-Desktops im Rechenzentrum. Für View Transfer Server gelten bestimmte Speicheranforderungen.

- Das Festplattenlaufwerk, auf dem Sie das Transfer Server-Repository speichern, muss über genügend Speicherplatz zum Speichern Ihrer statischen Image-Dateien verfügen. Image-Dateien sind View Composer-Basis-Images.
- View Transfer Server muss Zugriff auf die Datenspeicher besitzen, in denen die zu übertragenden Desktop-Festplatten gespeichert sind. Die Datenspeicher müssen von dem ESX-Host zugänglich sein, auf dem die virtuelle View Transfer Server-Maschine ausgeführt wird.
- View Transfer Server kann bis zu 60 Festplatten gleichzeitig übertragen.

  Während eines Übertragungsvorgangs wird die virtuelle Festplatte eines lokalen Desktops auf dem View Transfer Server gemountet. Die virtuelle View Transfer Server-Maschine verfügt über vier SCSI-Controller mit je 15 Slots. Diese Konfiguration ermöglicht es, dass in einem Vorgang bis zu 60 Festplatten mit der virtuellen Maschine verknüpft werden.
- Da lokale Desktops vertrauliche Benutzerdaten enthalten können, müssen die Daten während der Übertragung über das Netzwerk verschlüsselt werden.

  In View Administrator können Sie für jede View Connection Server-Instanz Sicherheitsoptionen für die Datenübertragung konfigurieren. Zum Konfigurieren dieser Optionen in View Administrator klicken Sie auf **[View Configuration (Konfiguration anzeigen)] > [Servers (Server)]** , wählen Sie eine View Connection Server-Instanz und klicken Sie auf **[Edit (Bearbeiten)]** .
- Beim Hinzufügen von View Transfer Server zu View Manager wird die DRS-Automatisierungsrichtlinie (Distributed Resource Scheduler) auf **[Manual (Manuell)]** eingestellt, wodurch DRS deaktiviert wird.

  Um eine View Transfer Server-Instanz auf einen anderen ESX-Host oder -Datenspeicher zu migrieren, müssen Sie die Instanz vor Beginn der Migration in den Wartungsmodus setzen.

  Wenn View Transfer Server aus View Manager entfernt wird, wird die DRS-Automatisierungsrichtlinie auf den Wert zurückgesetzt, auf den sie vor dem Hinzufügen von View Transfer Server zu View Manager festgelegt war.

Systemanforderungen für Clientkomponenten

2

Systeme, auf denen View-Clientkomponenten ausgeführt werden, müssen bestimmte Hardware- und Softwareanforderungen erfüllen.

Dieses Kapitel behandelt die folgenden Themen:

- „Unterstützte Betriebssysteme für View Agent“, auf Seite 15
- „Unterstützte Betriebssysteme für View Client und View Client with Local Mode“, auf Seite 16
- „Hardwareanforderungen für Desktops im lokalen Modus“, auf Seite 16
- „Clientbrowseranforderungen für View Portal“, auf Seite 18
- „Unterstützung für Remote-Anzeigeprotokoll und -Software“, auf Seite 18
- „Adobe Flash-Anforderungen“, auf Seite 22
- „Anforderungen für die Smartcard-Authentifizierung“, auf Seite 22

Unterstützte Betriebssysteme für View Agent

Die View Agent-Komponente bietet Unterstützung für Sitzungsverwaltung, einmalige Anmeldung (Single Sign-On, SSO) und Geräteumleitung. Sie müssen View Agent auf allen virtuellen Maschinen, physischen Systemen und Terminalservern installieren, die mit View Manager verwaltet werden.

Tabelle 2-1 listet die für View Agent unterstützten Betriebssysteme auf.

Tabelle 2-1. Betriebssystemunterstützung für View Agent

Gastbetriebssystem	Version	Edition	Service Pack
Windows 7	32-Bit und 64-Bit	Enterprise und Professional	–
Windows Vista	32-Bit	Business und Enterprise	SP1 und SP2
Windows XP	32-Bit	Professional	SP3
Windows 2008 R2 Terminal Server	64-Bit	Standard	–
Windows 2008 Terminal Server	64-Bit	Standard	SP2
Windows 2003 R2 Terminal Server	32-Bit	Standard	SP2
Windows 2003 Terminal Server	32-Bit	Standard	SP2

Wichtig Bei Verwendung von Windows 7 in einer virtuellen Maschine muss diese auf einem ESX 4.0- oder ESX 4.1-Server gehostet werden. Für ESX 4.0 ist die Version ESX 4.0 Update 2 oder höher erforderlich. Für ESX 4.1 ist die Version ESX 4.1 oder höher erforderlich.

Unterstützte Betriebssysteme für View Client und View Client with Local Mode

Benutzer führen View Client aus, um eine Verbindung mit ihren View-Desktops herzustellen. Sie müssen View Client oder View Client with Local Mode auf einem unterstützten Betriebssystem installieren.

Tabelle 2-2 listet die für View Client unterstützten Betriebssysteme auf.

Tabelle 2-2. Betriebssystemunterstützung für View Client

Betriebssystem	Version	Edition	Service Pack
Windows 7	32-Bit und 64-Bit	Home, Enterprise, Professional und Ultimate	–
Windows XP	32-Bit	Home und Professional	SP3
Windows Vista	32-Bit	Home, Business, Enterprise und Ultimate	SP1 und SP2
Mac OS X Leopard 10.5	–	–	–
Mac OS X Snow Leopard 10.6	–	–	–

WICHTIG View Client with Local Mode wird nur auf Windows-Systemen und ausschließlich auf physischen Computern unterstützt. Außerdem muss Ihre VMware-Lizenz zur Nutzung dieser Funktion View Client with Local Mode enthalten.

View Client with Local Mode ist die vollständig unterstützte Funktion, die in früheren Versionen eine experimentelle Funktion mit dem Namen View Client with Offline Desktop war.

Ein Windows 7- oder Windows Vista-View-Desktop, der auf einem ESX 3.5-Host erstellt wird, kann keine 3D- und Windows Aero-Effekte erzeugen. Diese Einschränkung gilt auch dann, wenn der Desktop zur lokalen Nutzung auf einem Windows 7- oder Windows Vista-Clientcomputer ausgecheckt wird. Windows Aero- und 3D-Effekte sind nur verfügbar, wenn der View-Desktop mittels vSphere 4.x erstellt wird.

HINWEIS VMware-Partner bieten Thin Client-Geräte für VMware View-Bereitstellungen an. Die Funktionen und Linux-Betriebssysteme, die für das jeweilige Thin Client-Gerät verfügbar sind, werden durch den Hersteller, das Modell und die Konfiguration festgelegt, die ein Unternehmen verwendet. Informationen zu Herstellern und Modellen für Thin Client-Geräte finden Sie im *Thin Client Compatibility Guide* (Thin Client-Kompatibilitätsleitfaden), der auf der VMware-Website zur Verfügung steht.

Hardwareanforderungen für Desktops im lokalen Modus

Wenn Sie einen View-Desktop zur Verwendung auf Ihrem lokalen Computer auschecken, muss die Hardware auf dem Clientcomputer sowohl das lokale System als auch die virtuelle Maschine unterstützen, die nun darauf ausgeführt wird.

PC-Hardware

Tabelle 2-3 beschreibt die Hardwareanforderungen für verschiedene View-Desktop-Betriebssysteme.

Tabelle 2-3. Prozessoranforderungen

Clientcomputeranforderung	Beschreibung
PC	Standardmäßiges x86-System oder x86-System mit 64-Bit-Kompatibilität
Anzahl von CPUs	Multiprozessorsysteme werden unterstützt

Tabelle 2-3. Prozessoranforderungen (Fortsetzung)

Clientcomputeranforderung	Beschreibung
CPU-Geschwindigkeit	Für einen lokalen Windows XP-Desktop 1,3 GHz oder schneller; 1,6 GHz empfohlen Für einen Windows 7-Desktop 1,6 GHz oder schneller; für Aero-Effekte 2,2 GHz oder schneller
Intel-Prozessoren	Pentium 4-, Pentium M- (mit PAE), Core-, Core 2-, Core i3-, Core i5- und Core i7-Prozessoren Für Windows 7-Aero: Intel-Dual-Core
AMD-Prozessoren	Athlon, Athlon MP, Athlon XP, Athlon 64, Athlon X2, Duron, Opteron, Turion X2, Turion 64, Sempron, Phenom und Phenom II Für Windows 7-Aero: Althon 4200+ und höher
64-Bit-Betriebssysteme	Intel Pentium 4- und Core 2- sowie Core i7-Prozessoren mit EM64T und Intel Virtualization Technology Die meisten AMD64-Prozessoren (ausgenommen Revision C Opteron-Prozessoren)
Grafikprozessor für Windows 7-Aero	nVidia GeForce 8800GT und höher ATI Radeon HD 2600 und höher

Festplattenspeicher

Bei Verwendung eines Standard-Setups für das Betriebssystem im View-Desktop entsprechen die tatsächlichen Anforderungen an den Festplattenspeicherplatz etwa den Anforderungen für die Installation und die Ausführung von Betriebssystem und Anwendungen auf einem physischen Computer.

Beispielsweise empfiehlt Microsoft 16 GB Festplattenspeicher für einen Computer, auf dem eine 32-Bit-Version von Windows 7 ausgeführt wird. Wenn Sie eine 16 GB große virtuelle Festplatte für eine virtuelle 32-Bit-Windows 7-Maschine konfigurieren, wird nur der tatsächlich verwendete Speicherplatz heruntergeladen, wenn Sie den lokalen Desktop auschecken. Für einen Desktop, dem 16 GB zugewiesen sind, beträgt die tatsächliche Downloadgröße möglicherweise 7 GB.

Nach dem Download des Desktops kann die Menge des verwendeten Speicherplatzes auf bis zu 16 GB ansteigen, wenn Sie eine Festplatte mit 16 GB konfiguriert haben. Da während der Replikation ein Snapshot erstellt wird, wird zusätzlich eine gleich große Menge an Speicherplatz benötigt. Wenn beispielsweise aktuell 7 GB Speicherplatz für den lokalen Desktop verwendet werden, belegt der Snapshot zusätzliche 7 GB auf dem Clientcomputer.

IDE- und SCSI-Festplattenlaufwerke werden unterstützt.

Arbeitsspeicher

Sie benötigen genügend Arbeitsspeicher zur Ausführung des Hostbetriebssystems auf dem Clientcomputer sowie die erforderliche Arbeitsspeicherkapazität für das Betriebssystem des View-Desktops und Anwendungen auf dem Clientcomputer und dem View-Desktop. VMware empfiehlt für Windows XP und Windows Vista 2 GB oder mehr, für Windows 7 werden 3 GB oder mehr empfohlen. Weitere Informationen zu den Arbeitsspeicheranforderungen finden Sie in der Dokumentation zu Ihrem Gastbetriebssystem sowie in der Anwendungsdokumentation.

Die Arbeitsspeichergröße, die Sie allen virtuellen Maschinen auf einem einzelnen Computer insgesamt zuweisen können, wird allein durch die RAM-Größe auf dem Computer begrenzt. Die maximale Arbeitsspeichergröße für jeden View-Desktop beträgt auf 32-Bit-Clientcomputern 8 GB und auf 64-Bit-Clientcomputern 32 GB.

Anzeige

Es wird ein 32-Bit-Anzeigeadapter empfohlen. 3D-Benchmarks, z.B. 3DMark '06, werden möglicherweise nicht ordnungsgemäß oder überhaupt nicht gerendert, wenn virtuelle Windows Vista- oder Windows 7-Maschinen auf einigen Grafikhardwareprodukten ausgeführt werden.

Zur Wiedergabe von Videos mit 720p oder mehr ist ein Multiprozessorsystem erforderlich.

Die CPU- und Grafikprozessoranforderungen zur Unterstützung von Windows 7-Aero sind in der Tabelle unter „PC-Hardware“, auf Seite 16 aufgeführt.

Clientbrowseranforderungen für View Portal

Sie können von einem Clientsystem aus zu einer View Connection Server-Instanz navigieren und über View Portal einen Mac-basierten View Client, einen Windows-basierten View Client oder View Client with Local Mode installieren. Bei Verwendung von Internet Explorer gibt View Portal an, wann eine neue Version von View Client zum Download bereitsteht.

Zur Verwendung von View Portal müssen Sie über einen der folgenden Webbrowser verfügen:

- Internet Explorer 7
- Internet Explorer 8
- Firefox 3.0
- Firefox 3.5

Wenn Sie Internet Explorer verwenden und View Client bereits installiert ist, können Sie ein Upgrade ausführen, wenn eine neuere View Connection Server-Version verfügbar ist als diejenige, die auf dem Clientgerät installiert ist. Wenn die Version mit der auf dem Clientgerät übereinstimmt, startet View Portal den auf dem lokalen System installierten View Client.

HINWEIS View Portal bietet keine Unterstützung für Linux. Für Linux wird ein nativer Client nur über zertifizierte VMware-Partner zur Verfügung gestellt.

Unterstützung für Remote-Anzeigeprotokoll und -Software

Remote-Anzeigeprotokolle und -Software bieten über eine Netzwerkverbindung Zugriff auf Desktops der Remote-Computer. View Client unterstützt Microsoft Remote Desktop Protocol (RDP), PCoIP von VMware und die RGS-Anzeigeprotokolle (Remote Graphics Software) von Hewlett-Packard.

- VMware View mit PCoIP auf Seite 19

  PCoIP ermöglicht ein optimales Desktop-Erlebnis bei der Bereitstellung der gesamten Desktop-Umgebung, einschließlich Anwendungen, Bildern sowie Audio- und Videoinhalten für eine große Anzahl an Benutzern im LAN oder im gesamten WAN. PCoIP kann längere Wartezeiten oder eine Verringerung der Bandbreite kompensieren und so sicherstellen, dass Endbenutzer ungeachtet der Netzwerkbedingungen weiter produktiv arbeiten können.

- Microsoft RDP auf Seite 20

  Microsoft Remotedesktopverbindung (Remote Desktop Connection, RDC) verwendet für die Übertragung von Daten RDP. RDP ist ein Mehrkanalprotokoll, das einem Benutzer die Remote-Verbindung mit einem Computer ermöglicht.

- HP RGS-Software auf Seite 21

  View Client unterstützt Desktop-Verbindungen mit HP RGS als Anzeigeprotokoll bei der Verbindungsherstellung mit HP Blade-PCs, HP Workstations und HP Blade Workstations. HP RGS gehört nicht zum Lieferumfang von View, und VMware bietet keine Lizenzen für HP RGS an. Wenden Sie sich an Hewlett-Packard, um eine Kopie von HP RGS 5.2.5 zur Verwendung mit VMware View zu lizenzieren.

- MMR (Multimedia Redirection) auf Seite 21

  Die MMR-Funktion (Multimedia Redirection) sendet Multimediadaten unter Verwendung eines virtuellen RDP-Kanals (Remote Desktop Protocol) direkt an den Client.

VMware View mit PCoIP

PCoIP ermöglicht ein optimales Desktop-Erlebnis bei der Bereitstellung der gesamten Desktop-Umgebung, einschließlich Anwendungen, Bildern sowie Audio- und Videoinhalten für eine große Anzahl an Benutzern im LAN oder im gesamten WAN. PCoIP kann längere Wartezeiten oder eine Verringerung der Bandbreite kompensieren und so sicherstellen, dass Endbenutzer ungeachtet der Netzwerkbedingungen weiter produktiv arbeiten können.

PCoIP wird als Anzeigeprotokoll für View-Desktops mit virtuellen Maschinen und physischen Computern unterstützt, die Teradici-Hostkarten enthalten.

PCoIP-Funktionen

Zu den wichtigsten Funktionen von PCoIP zählen:

- Remote-Verbindungen, die virtuelle private Netzwerke (VPNs) verwenden, werden unterstützt.
- Verbindungen zu Windows-Desktops mit den in „Unterstützte Betriebssysteme für View Agent“, auf Seite 15 aufgeführten View Agent-Betriebssystemversionen werden unterstützt.
- Verbindungen von Windows-Clients mit den in „Unterstützte Betriebssysteme für View Agent“, auf Seite 15 aufgeführten View Agent-Betriebssystemversionen werden unterstützt.
- Für Windows XP- und Vista-Clients wird die MMR-Funktion (Multimedia Redirection) unterstützt.
- Die USB-Umleitung wird unterstützt.
- Die Reduzierung der Adobe Flash-Bandbreitennutzung wird unterstützt.
- Eine Audioumleitung mit dynamischer Anpassung der Audioqualität für LAN und WAN wird unterstützt.
- Mehrere Monitore werden unterstützt. Sie können bis zu vier Monitore einsetzen und die Auflösung jedes Monitors einzeln festlegen, wobei eine Einstellung auf bis zu 1920 x 1200 pro Anzeigegerät möglich ist. Drehung des Monitors (Pivot-Funktion) und automatische Anpassung werden ebenfalls unterstützt.
- Unterstützung von 32-Bit-Farben für virtuelle Anzeigegeräte.
- ClearType-Schriftarten werden unterstützt.
- Das Kopieren und Einfügen von Text zwischen dem lokalen System und dem Desktop wird unterstützt. Sie können jedoch keine Systemobjekte wie Ordner und Dateien zwischen den Systemen kopieren und einfügen.

Videoqualität

480p-formatiertes Video Die Videowiedergabe mit 480p oder niedriger bei nativen Auflösungen ist möglich, wenn der View-Desktop über eine einzige virtuelle CPU verfügt. Wenn Sie unter Windows 7 eine Videowiedergabe in hoch auflösendem Flash- oder im Vollbildmodus wünschen, erfordert der Desktop eine duale virtuelle CPU.

720p-formatiertes Video Die Videowiedergabe mit 720p bei nativen Auflösungen ist möglich, wenn der View-Desktop über eine duale virtuelle CPU verfügt. Bei der 720p-Videowiedergabe in hoch auflösendem oder Vollbildmodus könnte die Leistung beeinträchtigt sein.

1080p-formatiertes Video Wenn der View-Desktop über eine duale virtuelle CPU verfügt, können Sie 1080p-formatiertes Video wiedergeben, obgleich der Media Player möglicherweise auf eine kleinere Fenstergröße angepasst werden muss.

PCoIP-Einschränkungen

PCoIP weist folgende Einschränkung auf: View Client-Computer, die PCoIP verwenden, können sich mit Sicherheitsservern verbinden, für PCoIP-Sitzungen mit dem Desktop wird der Sicherheitsserver jedoch ignoriert. PCoIP verwendet zum Streaming von Audio- und Videodaten UDP, Sicherheitsserver unterstützen jedoch ausschließlich TCP.

Empfohlene Einstellungen für das Gastbetriebssystem

Es werden die folgenden Einstellungen für das Gastbetriebssystem empfohlen:

- Für Windows XP-Desktops: 768 MB RAM oder mehr und eine einzige CPU
- Für Windows 7-Desktops: 1 GB RAM und eine duale CPU

Anforderungen an die Clienthardware

Folgende Clienthardwareanforderungen müssen erfüllt werden:

- Prozessorgeschwindigkeit: 800 MHz oder schneller
- x86-basierter Prozessor mit SSE2-Erweiterungen.
- Informationen zum Festlegen der Arbeitsspeichergröße für bestimmte Monitorkonfigurationen finden Sie im *Planungshandbuch für die VMware View-Architektur*.

Microsoft RDP

Microsoft Remotedesktopverbindung (Remote Desktop Connection, RDC) verwendet für die Übertragung von Daten RDP. RDP ist ein Mehrkanalprotokoll, das einem Benutzer die Remote-Verbindung mit einem Computer ermöglicht.

Nachfolgend werden RDP-bezogene Anforderungen und Überlegungen für unterschiedliche Windows-Betriebssysteme und -Funktionen vorgestellt.

- Für Windows XP- und Windows XPe-Systeme sollten Sie Microsoft RDC 6.x verwenden.
- Bei Windows Vista gehört RDC 6.x zum Lieferumfang.
- Windows 2000 unterstützt RDC 5.0. RDC 6.x wird von Windows 2000 nicht unterstützt.
- Zur Nutzung mehrerer Monitore müssen Sie RDC 6.0 oder höher verwenden.

- Für virtuelle Windows XP-Maschinen müssen Sie die RDP-Patches installieren, die in den Knowledgebase-Artikeln 323497 und 884020 aufgeführt sind. Wenn Sie die RDP-Patches nicht installieren, wird möglicherweise ein Windows Socket-Fehler auf dem Client angezeigt.
- Das View Agent-Installationsprogramm konfiguriert die lokale Firewall-Regel für eingehende RDP-Verbindungen entsprechend dem aktuellen RDP-Port des Hostbetriebssystems (üblicherweise 3389). Wenn Sie die RDP-Portnummer ändern, müssen Sie die dazugehörigen Firewall-Regeln ändern.

RDC 6.1 steht auf der Microsoft-Website zum Download zur Verfügung.

HP RGS-Software

View Client unterstützt Desktop-Verbindungen mit HP RGS als Anzeigeprotokoll bei der Verbindungsherstellung mit HP Blade-PCs, HP Workstations und HP Blade Workstations. HP RGS gehört nicht zum Lieferumfang von View, und VMware bietet keine Lizenzen für HP RGS an. Wenden Sie sich an Hewlett-Packard, um eine Kopie von HP RGS 5.2.5 zur Verwendung mit VMware View zu lizenzieren.

HP RGS umfasst eine serverseitige Komponente, den RGS-Sender, sowie eine clientseitige Komponente, den RGS-Empfänger. Um VMware View für die Verwendung von HP RGS konfigurieren zu können, muss der HP RGS-Sender auf dem Betriebssystem des Remote-Desktops und der HP RGS-Empfänger auf dem Desktop installiert werden. Installieren Sie RGS USB weder auf dem Sender noch auf dem Empfänger.

Sie müssen die RGS-Senderanwendung bzw. den Port in Ihrer Firewall-Software als Ausnahme hinzufügen. Der Standard-RGS-Port lautet 42966. Informationen zur Installation und Konfiguration von HP RGS-Komponenten finden Sie in der HP RGS-Dokumentation auf der Website von Hewlett-Packard.

HP RGS weist folgende Einschränkungen auf:

- Verbindungen mit virtuellen Maschinen werden nicht unterstützt.
- Vista-Desktops werden nicht unterstützt.
- Tunnelverbindungen werden nicht unterstützt. Nur direkte Verbindungen werden unterstützt.
- Smartcards werden nicht unterstützt.
- Mehrere Monitore werden nicht unterstützt.
- View Portal unterstützt keine RGS-Verbindungen.
- Linux-Thin Clients bieten keine Unterstützung für RGS-Verbindungen.

MMR (Multimedia Redirection)

Die MMR-Funktion (Multimedia Redirection) sendet Multimediadaten unter Verwendung eines virtuellen RDP-Kanals (Remote Desktop Protocol) direkt an den Client.

View Client und View Client with Local Mode unterstützen MMR auf den folgenden Betriebssystemen:

- Windows XP
- Windows XP Embedded
- Windows Vista

Die MMR-Funktion unterstützt die Mediendateiformate, die das Clientsystem unterstützt, da auf dem Client lokale Decoder vorhanden sein müssen. Zu den unterstützten Dateiformaten zählen u.a. MPEG2, WMV, AVI und WAV.

Arbeiten Sie zum Erzielen optimaler Qualität mit Windows Media Player 10 oder höher, und installieren Sie das Programm sowohl auf dem lokalen Computer als auch dem Clientzugriffsgerät sowie dem View-Desktop.

Sie müssen den MMR-Port in Ihrer Firewall-Software als Ausnahme hinzufügen. Der standardmäßige Port für MMR lautet 9427.

Hinweis Die View Client-Hardware zur Videoanzeige muss Overlay-Unterstützung bieten, damit MMR ordnungsgemäß funktioniert.

Adobe Flash-Anforderungen

Sie können die durch Adobe Flash-Inhalte in View-Desktop-Sitzungen verwendete Bandbreite reduzieren. Durch diese Reduzierung kann die Browsing-Leistung insgesamt sowie die Reaktionsfähigkeit anderer im Desktop ausgeführten Anwendungen verbessert werden.

Die Adobe Flash-Bandbreite lässt sich ausschließlich für Internet Explorer-Sitzungen unter Microsoft Windows sowie für Adobe Flash 9 und 10 reduzieren. Um die Einstellungen zur Reduzierung der Adobe Flash-Bandbreite zu nutzen, darf Adobe Flash nicht im Vollbildmodus ausgeführt werden.

Anforderungen für die Smartcard-Authentifizierung

Clientsysteme, die eine Smartcard für die Benutzerauthentifizierung verwenden, müssen bestimmte Anforderungen erfüllen.

Für jedes Clientsystem, das zur Benutzerauthentifizierung eine Smartcard verwendet, gelten die folgenden Software- und Hardwareanforderungen:

- View Client
- Ein Windows-kompatibler Smartcard-Leser
- Smartcard-Middleware
- Produktspezifische Anwendungstreiber

Sie müssen auf den View-Desktops zusätzlich produktspezifische Anwendungstreiber installieren.

VMware View unterstützt Smartcards und Smartcard-Leser, die einen PKCS#11- oder Microsoft CryptoAPI-Anbieter verwenden. Optional können Sie das ActivClient-Softwarepaket von ActivIdentity installieren, das Tools zur Interaktion mit Smartcards bereitstellt.

Benutzer, die sich mithilfe von Smartcards authentifizieren, müssen über ein Smartcard- oder USB-Smartcard-Token verfügen, und jede Smartcard muss ein Benutzerzertifikat enthalten.

Zum Installieren von Zertifikaten auf einer Smartcard müssen Sie einen Computer einrichten, der als Registrierungsstelle fungiert. Dieser Computer muss Smartcards für Benutzer ausgeben können und Mitglied der Domäne sein, für die Sie Zertifikate ausgeben.

Wichtig Wenn Sie eine Smartcard anmelden, können Sie die Schlüsselgröße des resultierenden Zertifikats auswählen. Um Smartcards mit lokalen Desktops zu verwenden, müssen Sie während der Smartcard-Anmeldung eine 1024-Bit- oder 2048-Bit-Schlüsselgröße auswählen. Zertifikate mit 512-Bit-Schlüsseln werden nicht unterstützt.

Die Microsoft TechNet-Website enthält ausführliche Informationen zu Planung und Implementierung der Smartcard-Authentifizierung für Windows-Systeme.

Informationen zu Aufgaben, die Sie möglicherweise beim Implementieren der Smartcard-Authentifizierung mit View im Active Directory durchführen müssen, finden Sie unter „Vorbereiten von Active Directory für die Smartcard-Authentifizierung“, auf Seite 27.

Die Smartcard-Authentifizierung wird von View Client für Mac und View Administrator nicht unterstützt. Ausführliche Informationen zur Smartcard-Unterstützung finden Sie im *Planungshandbuch für die VMware View-Architektur*.

Vorbereiten von Active Directory 3

View nutzt die vorhandene Microsoft Active Directory-Infrastruktur für die Benutzerauthentifizierung und -verwaltung. Zur Vorbereitung von Active Directory auf die Verwendung mit View müssen verschiedene Aufgaben ausgeführt werden.

Dieses Kapitel behandelt die folgenden Themen:

- „Konfigurieren von Domänen und Vertrauensbeziehungen“, auf Seite 23
- „Erstellen einer OU für View-Desktops“, auf Seite 24
- „Erstellen von Organisationseinheiten und Gruppen für Clientkonten im Kiosk-Modus“, auf Seite 24
- „Erstellen von Gruppen für View-Benutzer“, auf Seite 25
- „Erstellen eines Benutzerkontos für vCenter Server“, auf Seite 25
- „Erstellen eines Benutzerkontos für View Composer“, auf Seite 25
- „Konfigurieren der Richtlinie „Restricted Groups (Eingeschränkte Gruppen)““, auf Seite 26
- „Verwenden von Gruppenrichtlinien-ADM-Vorlagendateien für View“, auf Seite 26
- „Vorbereiten von Active Directory für die Smartcard-Authentifizierung“, auf Seite 27

Konfigurieren von Domänen und Vertrauensbeziehungen

Sie müssen jeden View Connection Server-Host zu einer Active Directory-Domäne hinzufügen. Bei dem Host darf es sich nicht um einen Domänencontroller handeln. Sie platzieren View-Desktops in derselben Domäne wie den View Connection Server-Host oder in einer Domäne, die über eine bidirektionale Vertrauensbeziehung mit der Domäne des View Connection Server-Hosts verfügt.

Sie können Benutzer und Gruppe in der Domäne des View Connection-Hosts für View-Desktops und -Pools berechtigen. Sie können außerdem Benutzer und Gruppen aus der Domäne des View Connection Server-Hosts als Administratoren in View Administrator festlegen. Um Benutzer oder Gruppen einer anderen Domäne zu berechtigen oder auszuwählen, müssen Sie eine bidirektionale Vertrauensbeziehung zwischen dieser Domäne und der Domäne des View Connection Server-Hosts einrichten.

Benutzer werden über Active Directory für die Domäne des View Connection Server-Hosts und eine beliebige Anzahl zusätzlicher Benutzerdomänen authentifiziert, mit denen eine Vertrauensstellung besteht.

Hinweis Da Sicherheitsserver nicht auf Authentifizierungs-Repositorys (einschließlich Active Directory) zugreifen, müssen sie sich nicht in einer Active Directory-Domäne befinden.

Vertrauensbeziehungen und Domänenfilterung

Um zu ermitteln, auf welche Domänen zugegriffen werden kann, durchläuft eine View Connection Server-Instanz – beginnend bei der eigenen Domäne – die vorhandenen Vertrauensbeziehungen.

Bei einer kleinen, gut verbundenen Gruppe von Domänen kann View Connection Server umgehend eine vollständige Liste der Domänen abrufen. Die zum Erstellen der Liste benötigte Zeit steigt jedoch mit zunehmender Anzahl an Domänen oder bei einer weniger guten Verbindung zwischen den Domänen an. Die Liste kann auch Domänen enthalten, die Sie Benutzern nicht anbieten möchten, wenn sie sich mit ihren Desktops verbinden.

Über den Befehl `vdmadmin` können Sie eine Domänenfilterung konfigurieren, um die von einer View Connection Server-Instanz durchsuchten und dem Benutzer angezeigten Domänen einzuschränken. Weitere Informationen finden Sie im *VMware View-Administratorhandbuch*.

Erstellen einer OU für View-Desktops

Sie sollten eine Organisationseinheit (Organizational Unit, OU) speziell für Ihre View-Desktops erstellen. Eine OU ist ein Containerelement zur Unterteilung in Active Directory, das Benutzer, Gruppen, Computer oder andere OUs enthalten kann.

Um zu verhindern, dass Gruppenrichtlinieneinstellungen auf andere Windows-Server oder -Arbeitsstationen in derselben Domäne wie Ihre Desktops angewendet werden, können Sie ein Gruppenrichtlinienobjekt (Group Policy Object, GPO) für Ihre View Manager-Gruppenrichtlinien erstellen und es mit der OU verknüpfen, die Ihre View-Desktops enthält. Sie können die Steuerung der OU auch an untergeordnete Gruppen delegieren, beispielsweise an Serveroperatoren oder einzelne Benutzer.

Wenn Sie View Composer verwenden, erstellen Sie einen separaten Active Directory-Container für Linked-Clone-Desktops, der auf der OU für Ihre View-Desktops basiert. View-Administratoren, die in Active Directory OU-Administratorberechtigungen besitzen, können ohne Domänenadministratorberechtigungen Linked-Clone-Desktops bereitstellen. Wenn Sie in Active Directory die Anmeldeinformationen für Administratoren ändern, müssen Sie auch die Anmeldeinformationen in View Composer aktualisieren.

Weitere Informationen finden Sie im *VMware View-Administratorhandbuch*.

Erstellen von Organisationseinheiten und Gruppen für Clientkonten im Kiosk-Modus

Ein Client im Kiosk-Modus ist ein Thin Client oder ein PC mit eingeschränkten Funktionen, auf dem View Client ausgeführt wird, um die Verbindung mit einer View Connection Server-Instanz herzustellen und eine Remote-Desktop-Sitzung zu starten. Wenn Sie Clients im Kiosk-Modus konfigurieren, sollten Sie in Active Directory dedizierte Organisationseinheiten (Organizational Units, OUs) und Gruppen für diese Clients konfigurieren.

Durch das Erstellen von dedizierten OUs und Gruppen für Clientkonten im Kiosk-Modus werden Clientsysteme unterteilt, um sie vor einem unberechtigten Zugriff zu schützen. Gleichzeitig wird so die Konfiguration und Verwaltung der Clients vereinfacht.

Weitere Informationen finden Sie im *VMware View-Administratorhandbuch*.

Erstellen von Gruppen für View-Benutzer

Sie sollten in Active Directory Gruppen für unterschiedliche Arten von View-Benutzern erstellen. Beispielsweise können Sie eine Gruppe mit Namen "VMware View-Benutzer" für Ihre View-Desktop-Benutzer und eine weitere Gruppe namens "VMware View-Administratoren" für Benutzer erstellen, die View-Desktops verwalten.

Erstellen eines Benutzerkontos für vCenter Server

Sie müssen ein Benutzerkonto in Active Directory erstellen, um es mit vCenter Server einzusetzen. Geben Sie dieses Benutzerkonto an, wenn Sie eine vCenter Server-Instanz in View Administrator hinzufügen.

Das Benutzerkonto muss sich in derselben Domäne wie Ihr View Connection Server-Host oder in einer vertrauenswürdigen Domäne befinden. Wenn Sie View Composer verwenden, müssen Sie das Benutzerkonto zur lokalen Administratorengruppe auf dem vCenter Server-Computer hinzufügen.

Sie müssen dem Benutzerkonto Berechtigungen zum Ausführen bestimmter Vorgänge in vCenter Server erteilen. Wenn Sie View Composer verwenden, müssen Sie dem Benutzerkonto zusätzliche Berechtigungen erteilen. Weitere Informationen zur Konfiguration dieser Berechtigungen finden Sie unter „Konfigurieren von Benutzerkonten für vCenter Server und View Composer“, auf Seite 56.

Erstellen eines Benutzerkontos für View Composer

Wenn Sie View Composer verwenden, müssen Sie in Active Directory ein Benutzerkonto zur Verwendung mit View Composer erstellen. Dieses Konto ist für View Composer erforderlich, um Linked-Clone-Desktops zur Active Directory-Domäne hinzuzufügen.

Zur Gewährleistung der Sicherheit sollten Sie ein separates Benutzerkonto für View Composer erstellen. Durch das Erstellen eines separaten Kontos können Sie sicherstellen, dass keine zusätzlichen Berechtigungen für andere Zwecke gewährt werden. Sie können diesem Konto die Mindestberechtigungen erteilen, die zum Erstellen und Entfernen von Computerobjekten in einem festgelegten Active Directory-Container erforderlich sind. Beispielsweise sind für das View Composer-Konto nicht die Berechtigungen eines Domänenadministrators erforderlich.

Vorgehensweise

1 Erstellen Sie in Active Directory ein Benutzerkonto, das sich in derselben Domäne wie Ihr View Connection Server-Host oder in einer vertrauenswürdigen Domäne befindet.

2 Fügen Sie die Berechtigungen **[Create Computer Objects (Computerobjekte erstellen)]**, **[Delete Computer Objects (Computerobjekte löschen)]** und **[Write All Properties (Alle Eigenschaften schreiben)]** für das Konto in dem Active Directory-Container hinzu, in dem die Linked-Clone-Computerkonten erstellt werden bzw. in den die Linked-Clone-Computerkonten verschoben werden sollen.

   Die folgende Liste zeigt alle für das Benutzerkonto erforderlichen Berechtigungen, einschließlich der standardmäßig zugewiesenen Berechtigungen:

   - List Contents (Inhalt auflisten)
   - Read All Properties (Alle Eigenschaften lesen)
   - Write All Properties (Alle Eigenschaften schreiben)
   - Read Permissions (Berechtigungen lesen)
   - Create Computer Objects (Computerobjekte erstellen)
   - Delete Computer Objects (Computerobjekte löschen)

3 Stellen Sie sicher, dass die Berechtigungen für das Benutzerkonto für den Active Directory-Container und alle untergeordneten Objekte des Containers gelten.

Weiter

Geben Sie das Konto in View Administrator an, wenn Sie View Composer für vCenter Server konfigurieren und Linked-Clone-Desktop-Pools konfigurieren und bereitstellen.

Konfigurieren der Richtlinie „Restricted Groups (Eingeschränkte Gruppen)“

Um sich an einem View-Desktop anmelden zu können, müssen Benutzer der lokalen Gruppe **[Remote Desktop Users (Remote-Desktop-Benutzer)]** für den View-Desktop angehören. Sie können die Richtlinie **[Restricted Groups (Eingeschränkte Gruppen)]** in Active Directory dazu verwenden, um Benutzer oder Gruppen zur lokalen Gruppe der Remote-Desktop-Benutzer für jeden View-Desktop hinzuzufügen, der Ihrer Domäne angehört.

Die Richtlinie **[Restricted Groups (Eingeschränkte Gruppen)]** legt die lokale Gruppenmitgliedschaft für Computer in der Domäne so fest, dass sie mit den Mitgliedschaftseinstellungen in der Richtlinie **[Restricted Groups (Eingeschränkte Gruppen)]** übereinstimmt. Die Mitglieder Ihrer View-Desktop-Benutzergruppe werden stets der lokalen Gruppe **[Remote-Desktop-Benutzer]** für jeden View-Desktop hinzugefügt, den Sie Ihrer Domäne hinzufügen. Wenn Sie neue Benutzer hinzufügen, müssen Sie diese lediglich der Gruppe der View-Desktop-Benutzer hinzufügen.

Voraussetzungen

Erstellen Sie in Active Directory eine Gruppe für die View-Desktop-Benutzer in Ihrer Domäne.

Vorgehensweise

1 Wählen Sie auf dem Active Directory-Server **[Start] > [Administrative Tools (Verwaltung)] > [Active Directory Users and Computers (Active Directory-Benutzer und -Computer)]** .

2 Klicken Sie mit der rechten Maustaste auf die Domäne und wählen Sie **[Properties (Eigenschaften)]** .

3 Klicken Sie auf der Registerkarte **[Group Policy (Gruppenrichtlinie)]** auf **[Open (Öffnen)]** , um das Plug-In **[Group Policy Management (Gruppenrichtlinienverwaltung)]** zu öffnen.

4 Klicken Sie mit der rechten Maustaste auf **[Default Domain Policy (Standarddomänenrichtlinie)]** und anschließend auf **[Edit (Bearbeiten)]** .

5 Erweitern Sie den Abschnitt **[Computer Configuration (Computerkonfiguration)]** und öffnen Sie **[Windows Settings\Security Settings\Public Key Policies (Windows-Einstellungen\Sicherheitseinstellungen\Richtlinien für öffentliche Schlüssel)]** .

6 Klicken Sie mit der rechten Maustaste auf **[Restricted Groups (Eingeschränkte Gruppen)]** , wählen Sie **[Add Group (Gruppe hinzufügen)]** , und fügen Sie die Gruppe **[Remote Desktop Users (Remote-Desktop-Benutzer)]** hinzu.

7 Klicken Sie mit der rechten Maustaste auf die neue eingeschränkte Gruppe **[Remote Desktop Users (Remote-Desktop-Benutzer)]** und fügen Sie der Liste der Gruppenmitglieder Ihre View-Desktop-Benutzergruppe hinzu.

8 Klicken Sie auf **[OK]** , um Ihre Änderungen zu speichern.

Verwenden von Gruppenrichtlinien-ADM-Vorlagendateien für View

View umfasst verschiedene komponentenspezifische administrative Vorlagendateien für Gruppenrichtlinien (ADM-Vorlagendateien).

Während der View Connection Server-Installation werden die View-ADM-Vorlagendateien im *Installationsverzeichnis*\VMware\VMware View\Server\Extras\GroupPolicyFiles auf Ihrem View Connection Server-Host installiert. Sie müssen diese Dateien in ein Verzeichnis auf Ihrem Active Directory-Server kopieren.

Sie können View-Desktops optimieren und schützen, indem Sie die Richtlinieneinstellungen in diesen Dateien auf ein neues oder vorhandenes Gruppenrichtlinienobjekt (Group Policy Object, GPO) anwenden und das GPO mit der Organisationseinheit (Organizational Unit, OU) verknüpfen, die Ihre View-Desktops enthält.

Weitere Informationen zur Verwendung der View-Gruppenrichtlinieneinstellungen finden Sie im *VMware View-Administratorhandbuch*.

Vorbereiten von Active Directory für die Smartcard-Authentifizierung

Sie müssen in Active Directory möglicherweise bestimmte Aufgaben ausführen, wenn Sie die Smartcard-Authentifizierung implementieren.

- Hinzufügen von UPNs für Smartcard-Benutzer auf Seite 27

  Da sich die Smartcard-Anmeldung auf Benutzerprinzipalnamen (User Principal Names, UPNs) stützt, müssen die Active Directory-Konten von Benutzern, die sich in View per Smartcard authentifizieren, über einen gültigen UPN verfügen.

- Hinzufügen des Stammzertifikats zu den vertrauenswürdigen Stammzertifizierungsstellen auf Seite 28

  Wenn Sie eine Zertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Stammzertifikat zur Gruppenrichtlinie **[Trusted Root Certification Authorities (Vertrauenswürdige Stammzertifizierungsstellen)]** in Active Directory hinzufügen. Dieser Vorgang ist nicht erforderlich, wenn der Windows-Domänencontroller als Stammzertifizierungsstelle fungiert.

- Hinzufügen des Stammzertifikats zum Enterprise NTAuth-Speicher auf Seite 29

  Wenn Sie eine Zertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Stammzertifikat dem Enterprise NTAuth-Speicher in Active Directory hinzufügen. Dieser Vorgang ist nicht erforderlich, wenn der Windows-Domänencontroller als Stammzertifizierungsstelle fungiert.

Hinzufügen von UPNs für Smartcard-Benutzer

Da sich die Smartcard-Anmeldung auf Benutzerprinzipalnamen (User Principal Names, UPNs) stützt, müssen die Active Directory-Konten von Benutzern, die sich in View per Smartcard authentifizieren, über einen gültigen UPN verfügen.

Wenn sich der Smartcard-Benutzer in einer anderen Domäne befindet als derjenigen, von der Ihr Stammzertifikat ausgegeben wurde, müssen Sie den UPN des Benutzers auf den alternativen Antragstellernamen (Subject Alternative Name, SAN) festlegen, der im Stammzertifikat der vertrauenswürdigen Zertifizierungsstelle angegeben ist. Wenn Ihr Stammzertifikat von einem anderen Server in der aktuellen Domäne des Smartcard-Benutzers ausgegeben wurde, ist eine Änderung des Benutzer-UPNs nicht erforderlich.

Hinweis Sie müssen möglicherweise den UPN für integrierte Active Directory-Konten angeben, selbst wenn das Zertifikat von derselben Domäne ausgegeben wurde. Für integrierte Konten, einschließlich des Administratorkontos, ist standardmäßig kein UPN festgelegt.

Voraussetzungen

- Sie können den alternativen Antragstellernamen (SAN) abrufen, indem Sie im Stammzertifikat der vertrauenswürdigen Zertifizierungsstelle die Zertifikateigenschaften anzeigen.
- Wenn das Dienstprogramm ADSI-Editor nicht auf Ihrem Active Directory-Server zur Verfügung steht, laden Sie die Windows-Supporttools von der Microsoft-Website herunter.

Vorgehensweise

1 Starten Sie auf Ihrem Active Directory-Server das Dienstprogramm ADSI-Editor.

2 Erweitern Sie im linken Fensterbereich die Domäne, in der sich der Benutzer befindet, und doppelklicken Sie auf `CN=Users`.

3 Klicken Sie im rechten Fensterbereich mit der rechten Maustaste auf den Benutzer und anschließend auf **[Properties (Eigenschaften)]** .

4 Doppelklicken Sie auf das Attribut `userPrincipalName` und geben Sie den SAN-Wert für das Zertifikat der vertrauenswürdigen Zertifizierungsstelle ein.

5 Klicken Sie auf **[OK]** , um die Attributeinstellung zu speichern.

Hinzufügen des Stammzertifikats zu den vertrauenswürdigen Stammzertifizierungsstellen

Wenn Sie eine Zertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Stammzertifikat zur Gruppenrichtlinie **[Trusted Root Certification Authorities (Vertrauenswürdige Stammzertifizierungsstellen)]** in Active Directory hinzufügen. Dieser Vorgang ist nicht erforderlich, wenn der Windows-Domänencontroller als Stammzertifizierungsstelle fungiert.

Vorgehensweise

1 Wählen Sie auf dem Active Directory-Server **[Start] > [All Programs (Alle Programme)] > [Administrative Tools (Verwaltung)] > [Active Directory Users and Computers (Active Directory-Benutzer und -Computer)]** .

2 Klicken Sie mit der rechten Maustaste auf die Domäne und anschließend auf **[Properties (Eigenschaften)]** .

3 Klicken Sie auf der Registerkarte **[Group Policy (Gruppenrichtlinie)]** auf **[Open (Öffnen)]** , um das Plug-In **[Group Policy Management (Gruppenrichtlinienverwaltung)]** zu öffnen.

4 Klicken Sie mit der rechten Maustaste auf **[Default Domain Policy (Standarddomänenrichtlinie)]** und anschließend auf **[Edit (Bearbeiten)]** .

5 Erweitern Sie den Abschnitt **[Computer Configuration (Computerkonfiguration)]** und öffnen Sie **[Windows Settings\Security Settings\Public Key Policies (Windows-Einstellungen\Sicherheitseinstellungen\Richtlinien für öffentliche Schlüssel)]** .

6 Klicken Sie mit der rechten Maustaste auf **[Trusted Root Certification Authorities (Vertrauenswürdige Stammzertifizierungsstellen)]** und wählen Sie **[Import (Importieren)]** .

7 Folgen Sie den Anweisungen des Assistenten, um das Zertifikat zu importieren. Klicken Sie anschließend auf **[OK]** .

8 Schließen Sie den Gruppenrichtlinienverwaltungs-Editor.

Alle Systeme in der Domäne verfügen nun über eine Kopie des Zertifikats in ihrem vertrauenswürdigen Stammspeicher.

Hinzufügen des Stammzertifikats zum Enterprise NTAuth-Speicher

Wenn Sie eine Zertifizierungsstelle verwenden, um Zertifikate für die Smartcard-Anmeldung oder für Domänencontroller auszugeben, müssen Sie das Stammzertifikat dem Enterprise NTAuth-Speicher in Active Directory hinzufügen. Dieser Vorgang ist nicht erforderlich, wenn der Windows-Domänencontroller als Stammzertifizierungsstelle fungiert.

Vorgehensweise

- Verwenden Sie auf dem Active Directory-Server den Befehl `certutil`, um das Zertifikat im Enterprise NTAuth-Speicher zu veröffentlichen.

  Beispiel: **`certutil –dspublish –f`** ***`Pfad_zum_Zertifikat_der_Stammzertifizierungsstelle`*** **`NTAuthCA`**

Die Zertifizierungsstelle wird jetzt als vertrauenswürdig eingestuft und kann Zertifikate dieses Typs ausstellen.

Installieren von View Composer 4

Zur Verwendung von View Composer erstellen Sie eine View Composer-Datenbank, installieren den View Composer-Dienst auf dem vCenter Server-Computer und optimieren Ihre View-Infrastruktur zur Unterstützung von View Composer.

View Composer ist eine optionale Funktion. Installieren Sie View Composer, wenn Sie Linked-Clone-Desktop-Pools bereitstellen möchten.

Zu Installation und Verwendung der View Composer-Funktion benötigen Sie eine Lizenz.

Dieses Kapitel behandelt die folgenden Themen:

- „Vorbereiten einer View Composer-Datenbank“, auf Seite 31
- „Installieren des View Composer-Dienstes“, auf Seite 38
- „Konfigurieren der Infrastruktur für View Composer“, auf Seite 39

Vorbereiten einer View Composer-Datenbank

Sie müssen eine Datenbank und einen Datenquellennamen (Data Source Name, DSN) zum Speichern von View Composer-Daten erstellen.

Der View Composer-Dienst umfasst keine Datenbank. Falls weder auf dem vCenter Server-Computer noch an anderer Stelle in Ihrer Netzwerkumgebung eine Datenbankinstanz vorhanden ist, müssen Sie eine Datenbank installieren. Nach dem Installieren der Datenbankinstanz fügen Sie die View Composer-Datenbank zur Instanz hinzu.

Die View Composer-Datenbank speichert Informationen zu Verbindungen und Komponenten, die von View Composer verwendet werden:

- vCenter Server-Verbindungen
- Active Directory-Verbindungen
- Linked-Clone-Desktops, die von View Composer bereitgestellt werden
- Replikate, die von View Composer erstellt werden

Jede Instanz des View Composer-Dienstes muss über eine eigene View Composer-Datenbank verfügen. Mehrere View Composer-Dienste können eine View Composer-Datenbank nicht gemeinsam nutzen.

Eine Liste der unterstützten Datenbankversionen finden Sie unter „Datenbankanforderungen für View Composer“, auf Seite 10.

Befolgen Sie zum Hinzufügen einer View Composer-Datenbank zu einer installierten Datenbankinstanz eine dieser Vorgehensweisen.

- Erstellen einer SQL Server-Datenbank für View Composer auf Seite 32

  View Composer kann Informationen zu Linked-Clone-Desktops in einer SQL Server-Datenbank speichern. Sie erstellen eine View Composer-Datenbank, indem Sie sie zu SQL Server hinzufügen und eine ODBC-Datenquelle für die Datenbank konfigurieren.

- Erstellen einer Oracle 11g- oder Oracle 10g-Datenbank für View Composer auf Seite 34

  View Composer kann Informationen zu Linked-Clone-Desktops in einer Oracle 11g- oder Oracle 10g-Datenbank speichern. Sie erstellen eine View Composer-Datenbank, indem Sie sie zu einer vorhandenen Oracle 11g- oder Oracle 10g-Instanz hinzufügen und eine ODBC-Datenquelle für die Datenbank konfigurieren.

- Erstellen einer Oracle 9i-Datenbank für View Composer auf Seite 36

  View Composer kann Informationen zu Linked-Clone-Desktops in einer Oracle 9i-Datenbank speichern. Sie erstellen eine View Composer-Datenbank, indem Sie sie zu einer vorhandenen Oracle 9i-Instanz hinzufügen und eine ODBC-Datenquelle für die Datenbank konfigurieren.

Erstellen einer SQL Server-Datenbank für View Composer

View Composer kann Informationen zu Linked-Clone-Desktops in einer SQL Server-Datenbank speichern. Sie erstellen eine View Composer-Datenbank, indem Sie sie zu SQL Server hinzufügen und eine ODBC-Datenquelle für die Datenbank konfigurieren.

Hinzufügen einer View Composer-Datenbank zu SQL Server

Sie können einer vorhandenen Microsoft SQL Server-Instanz eine neue View Composer-Datenbank hinzufügen, um Linked-Clone-Daten für View Composer zu speichern.

Wenn die Datenbank sich auf demselben System befindet wie vCenter Server, können Sie als Sicherheitsmodell die integrierte Windows-Authentifizierung verwenden. Diese Authentifizierungsmethode kann nicht verwendet werden, wenn die Datenbank auf einem Remote-System vorliegt.

Voraussetzungen

- Stellen Sie sicher, dass eine unterstützte Version von SQL Server auf dem vCenter Server-Computer oder in Ihrer Netzwerkumgebung installiert ist. Weitere Informationen finden Sie unter „Datenbankanforderungen für View Composer“, auf Seite 10.
- Stellen Sie sicher, dass Sie SQL Server Management Studio oder SQL Server Management Studio Express zum Erstellen und Verwalten der Datenquelle verwenden. Sie können SQL Server Management Studio Express von der folgenden Website herunterladen und installieren.

  http://www.microsoft.com/downloadS/details.aspx?familyid=C243A5AE-4BD1-4E3D-94B8-5A0F62BF7796

Vorgehensweise

1. Wählen Sie auf dem vCenter Server-Computer **[Start] > [All Programs (Alle Programme)] > [Microsoft SQL Server 2008]** oder **[Microsoft SQL Server 2005]** .
2. Wählen Sie **[SQL Server Management Studio Express]** und stellen Sie eine Verbindung zur vorhandenen SQL Server-Instanz für vSphere Management her.
3. Klicken Sie im Objekt-Explorer mit der rechten Maustaste auf den Datenbankeneintrag und wählen Sie **[New Database (Neue Datenbank)]** .
4. Geben Sie im Dialogfeld **[New Database (Neue Datenbank)]** im Textfeld **[Database Name (Datenbankname)]** einen Namen ein.

   Beispiel: **`viewComposer`**

5 Klicken Sie auf **[OK]** .

SQL Server Management Studio Express fügt Ihre Datenbank zum Datenbankeneintrag im Objekt-Explorer hinzu.

6 Beenden Sie Microsoft SQL Server Management Studio Express.

Weiter

Folgen Sie den Anweisungen unter „Hinzufügen einer ODBC-Datenquelle zu SQL Server“, auf Seite 33.

Hinzufügen einer ODBC-Datenquelle zu SQL Server

Nachdem Sie eine View Composer-Datenbank zu SQL Server hinzugefügt haben, müssen Sie eine ODBC-Verbindung für die neue Datenbank konfigurieren, damit diese Datenquelle für den View Composer-Dienst sichtbar ist.

Bei den folgenden Anweisungen wird vorausgesetzt, dass Sie die ODBC-Datenquelle auf Windows Server 2003 SP1 konfigurieren. Wenn Sie die ODBC-Datenquelle auf Windows XP Professional SP2 konfigurieren, können einige der Schritte abweichen.

Voraussetzungen

Führen Sie die unter „Hinzufügen einer View Composer-Datenbank zu SQL Server“, auf Seite 32 beschriebenen Schritte aus.

Vorgehensweise

1 Wählen Sie auf dem vCenter Server-Computer **[Start] > [Administrative Tools (Verwaltung)] > [Data Source (ODBC) (Datenquellen (ODBC))]** .

2 Klicken Sie auf die Registerkarte **[System DSN (System-DSN)]** .

3 Klicken Sie auf **[Add (Hinzufügen)]** und wählen Sie in der angezeigten Liste den Eintrag **[SQL Native Client]** .

4 Klicken Sie auf **[Finish (Fertig stellen)]** .

5 Geben Sie im Assistenten Create a New Data Source to SQL Server setup (Neue Datenquelle für SQL Server erstellen) einen Namen und eine Beschreibung der View Composer-Datenbank ein.

Beispiel: **`ViewComposer`**

6 Geben Sie im Textfeld **[Server]** den Namen der SQL Server-Datenbank ein.

Verwenden Sie das Format <*Hostname*>\<*Servername*>, wobei <*Hostname*> für den Namen des Computers und <*Servername*> für die SQL Server-Instanz steht.

Beispiel: **`VCHOST1\SQLEXP_VIM`**

7 Klicken Sie auf **[Next (Weiter)]** .

8 Stellen Sie sicher, dass das Kontrollkästchen **[Connect to SQL Server to obtain default settings for the additional configuration options (Zum SQL Server verbinden, um Standardeinstellungen für die zusätzlichen Konfigurationsoptionen zu erhalten)]** aktiviert ist, und wählen Sie eine Authentifizierungsoption.

Option	Beschreibung
Windows NT authentication (Windows NT-Authentifizierung)	Wählen Sie diese Option, wenn Sie eine lokale Instanz von SQL Server verwenden. Diese Option wird auch als vertrauenswürdige Authentifizierung bezeichnet. Die Windows NT-Authentifizierung wird nur unterstützt, wenn SQL Server auf dem vCenter Server-Computer ausgeführt wird.
SQL Server authentication (SQL Server-Authentifizierung)	Wählen Sie diese Option, wenn Sie eine Remote-Instanz von SQL Server verwenden. Die Windows NT-Authentifizierung wird auf Remote-Computern mit SQL Server nicht unterstützt.

9 Klicken Sie auf **[Next (Weiter)]** .

10 Aktivieren Sie das Kontrollkästchen **[Change the default database to (Die Standarddatenbank ändern auf)]** und wählen Sie den Namen der View Composer-Datenbank in der Liste aus.

Beispiel: `ViewComposer`

11 Beenden und schließen Sie den Microsoft ODBC-Datenquellenadministrator.

Weiter

Installieren Sie den neuen View Composer-Dienst auf dem vCenter Server-Computer. Siehe „Installieren des View Composer-Dienstes“, auf Seite 38.

Erstellen einer Oracle 11g- oder Oracle 10g-Datenbank für View Composer

View Composer kann Informationen zu Linked-Clone-Desktops in einer Oracle 11g- oder Oracle 10g-Datenbank speichern. Sie erstellen eine View Composer-Datenbank, indem Sie sie zu einer vorhandenen Oracle 11g- oder Oracle 10g-Instanz hinzufügen und eine ODBC-Datenquelle für die Datenbank konfigurieren.

Hinzufügen einer View Composer-Datenbank zu Oracle 11g oder 10g

Sie können einer vorhandenen Oracle 11g- oder Oracle 10g-Instanz eine neue View Composer-Datenbank hinzufügen, um Linked-Clone-Daten für View Composer zu speichern.

Voraussetzungen

Stellen Sie sicher, dass auf dem vCenter Server-Computer eine unterstützte Version von Oracle 11g oder 10g installiert ist. Weitere Informationen finden Sie unter „Datenbankanforderungen für View Composer“, auf Seite 10.

Vorgehensweise

1 Starten Sie auf dem vCenter Server-Computer den **[Database Configuration Assistant (Datenbankkonfigurations-Assistent)]** .

Datenbankversion	Aktion
Oracle 11g	Wählen Sie **[Start]** > **[All Programs (Alle Programme)]** > **[Oracle-OraDb11g_home]** > **[Configuration and Migration Tools (Konfigurations- und Migrations-Tools)]** > **[Database Configuration Assistant (Datenbankkonfigurations-Assistent)]** .
Oracle 10g	Wählen Sie **[Start]** > **[All Programs (Alle Programme)]** > **[Oracle-OraDb10g_home]** > **[Configuration and Migration Tools (Konfigurations- und Migrations-Tools)]** > **[Database Configuration Assistant (Datenbankkonfigurations-Assistent)]** .

2 Wählen Sie auf der Seite **[Operation (Operation)]** die Option **[Create a database (Datenbank erstellen)]** und klicken Sie auf **[Next (Weiter)]** .

3 Wählen Sie auf der Seite **[Database Templates (Datenbankvorlagen)]** die Vorlage **[General Purpose or Transaction Processing (Allgemeiner Zweck oder Transaktionsverarbeitung)]** .

4 Geben Sie auf der Seite **[Database Identification (Datenbankidentifizierung)]** einen globalen Datenbanknamen und ein Präfix für die Oracle-Systemkennung (System Identifier, SID) ein.

Geben Sie der Einfachheit halber für beide Einstellungen denselben Wert an.

5 Klicken Sie auf der Seite **[Management Options (Verwaltungsoptionen)]** auf **[Next (Weiter)]** , um die Standardeinstellungen zu akzeptieren.

6 Wählen Sie auf der Seite **[Database Credentials (Datenbankanmeldeinformationen)]** die Option **[Use the Same Administrative Passwords for All Accounts (Dasselbe Verwaltungskennwort für alle Konten verwenden)]** und geben Sie ein Kennwort ein.

7 Klicken Sie auf den verbleibenden Konfigurationsseiten auf **[Next (Weiter)]** , um die Standardeinstellungen zu akzeptieren.

8 Vergewissern Sie sich, dass auf der Seite **[Creation Options (Erstellungsoptionen)]** die Option **[Create Database (Datenbank erstellen)]** aktiviert ist, und klicken Sie auf **[Finish (Fertig stellen)]** .

9 Überprüfen Sie die Optionen auf der Bestätigungsseite und klicken Sie auf **[OK]** .

Das Konfigurationstool erstellt die Datenbank.

10 Klicken Sie auf der Seite **[Database Creation Complete (Datenbankerstellung abgeschlossen)]** auf **[OK]** .

Weiter

Folgen Sie den Anweisungen unter „Hinzufügen einer ODBC-Datenquelle zu Oracle 11g oder 10g“, auf Seite 35.

Hinzufügen einer ODBC-Datenquelle zu Oracle 11g oder 10g

Nachdem Sie eine View Composer-Datenbank zu einer Oracle 11g- oder Oracle 10g-Instanz hinzugefügt haben, müssen Sie eine ODBC-Verbindung für die neue Datenbank konfigurieren, damit diese Datenquelle für den View Composer-Dienst sichtbar ist.

Bei den folgenden Anweisungen wird vorausgesetzt, dass Sie die ODBC-Datenquelle auf Windows Server 2003 SP1 konfigurieren. Wenn Sie die ODBC-Datenquelle auf Windows XP Professional SP2 konfigurieren, können einige der Schritte abweichen.

Voraussetzungen

Führen Sie die unter „Hinzufügen einer View Composer-Datenbank zu Oracle 11g oder 10g“, auf Seite 34 beschriebenen Schritte aus.

Vorgehensweise

1 Wählen Sie auf dem vCenter Server-Computer **[Start] > [Administrative Tools (Verwaltung)] > [Data Source (ODBC) (Datenquellen (ODBC))]** .

2 Wechseln Sie im Microsoft ODBC-Datenquellenadministrator zur Registerkarte **[System DSN (System-DSN)]** .

3 Klicken Sie auf **[Add (Hinzufügen)]** und wählen Sie in der angezeigten Liste den geeigneten Oracle-Treiber aus.

Beispiel: `OraDb11g_home`

4 Klicken Sie auf **[Finish (Fertig stellen)]** .

5 Geben Sie im Dialogfeld **[Oracle ODBC Driver Configuration (Oracle-ODBC-Treiberkonfiguration)]** einen DSN zur Verwendung mit View Composer, eine Beschreibung der Datenquelle sowie eine Benutzer-ID für die Verbindungsherstellung mit der Datenbank ein.

HINWEIS Sie verwenden den DSN bei der Installation des View Composer-Dienstes.

6 Wählen Sie als **[TNS Service Name (TNS-Dienstname)]** den globalen Datenbanknamen im Dropdown-Menü aus.

Der Assistent für die Oracle-Datenbankkonfiguration legt den globalen Datenbanknamen fest.

7 Zum Überprüfen der Datenquelle klicken Sie auf **[Test Connection (Verbindung testen)]** und anschließend auf **[OK]** .

Weiter

Installieren Sie den neuen View Composer-Dienst auf dem vCenter Server-Computer. Siehe „Installieren des View Composer-Dienstes“, auf Seite 38.

Erstellen einer Oracle 9i-Datenbank für View Composer

View Composer kann Informationen zu Linked-Clone-Desktops in einer Oracle 9i-Datenbank speichern. Sie erstellen eine View Composer-Datenbank, indem Sie sie zu einer vorhandenen Oracle 9i-Instanz hinzufügen und eine ODBC-Datenquelle für die Datenbank konfigurieren.

Hinzufügen einer View Composer-Datenbank zu Oracle 9i

Sie können einer vorhandenen Oracle 9i-Instanz eine neue View Composer-Datenbank hinzufügen, um Linked-Clone-Daten für View Composer zu speichern.

Voraussetzungen

Stellen Sie sicher, dass auf dem vCenter Server-Computer eine unterstützte Version von Oracle 9i installiert ist. Weitere Informationen finden Sie unter „Datenbankanforderungen für View Composer“, auf Seite 10.

Vorgehensweise

1 Wählen Sie auf dem vCenter Server-Computer **[Start] > [All Programs (Alle Programme)] > [Oracle-OraHome92] > [Configuration and Migration Tools (Konfigurations- und Migrations-Tools)] > [Database Configuration Assistant (Datenbankkonfigurations-Assistent)]** .

2 Wählen Sie auf der Seite **[Operation (Operation)]** die Option **[Create a database (Datenbank erstellen)]** und klicken Sie auf **[Next (Weiter)]** .

3 Wählen Sie auf der Seite **[Database Templates (Datenbankvorlagen)]** die Vorlage **[General Purpose (Allgemeiner Zweck)]** .

4 Geben Sie auf der Seite **[Database Identification (Datenbankidentifizierung)]** einen globalen Datenbanknamen und ein Präfix für die Oracle-Systemkennung (System Identifier, SID) ein.

Geben Sie der Einfachheit halber für beide Einstellungen denselben Wert an.

5 Wählen Sie auf der Seite **[Database Connection Options (Datenbankverbindungsoptionen)]** die Option **[Dedicated Server Mode (Dedizierter Servermodus)]** .

6 Klicken Sie auf den verbleibenden Konfigurationsseiten auf **[Next (Weiter)]** , um die Standardeinstellungen zu akzeptieren.

7 Vergewissern Sie sich, dass auf der Seite **[Creation Options (Erstellungsoptionen)]** die Option **[Create Database (Datenbank erstellen)]** aktiviert ist, und klicken Sie auf **[Finish (Fertig stellen)]** .

8 Überprüfen Sie die Optionen auf der Seite **[Summary (Übersicht)]** und klicken Sie auf **[OK]** .

Das Konfigurationstool erstellt die Datenbank.

9 Legen Sie Kennwörter für die Administratorkonten SYS und SYSTEM fest.

Sie verwenden das Konto SYSTEM, um die Datenquellenverbindung einzurichten.

Weiter

Folgen Sie den Anweisungen unter „Hinzufügen einer ODBC-Datenquelle zu Oracle 9i“, auf Seite 37.

Hinzufügen einer ODBC-Datenquelle zu Oracle 9i

Nachdem Sie eine View Composer-Datenbank zu einer Oracle 9i-Instanz hinzugefügt haben, müssen Sie eine ODBC-Verbindung für die neue Datenbank konfigurieren, damit diese Datenquelle für den View Composer-Dienst sichtbar ist.

Bei den folgenden Anweisungen wird vorausgesetzt, dass Sie die ODBC-Datenquelle auf Windows Server 2003 SP1 konfigurieren. Wenn Sie die ODBC-Datenquelle auf Windows XP Professional SP2 konfigurieren, können einige der Schritte abweichen.

Voraussetzungen

Führen Sie die unter „Hinzufügen einer View Composer-Datenbank zu Oracle 9i“, auf Seite 36 beschriebenen Schritte aus.

Vorgehensweise

1 Wählen Sie auf dem vCenter Server-Computer **[Start] > [Administrative Tools (Verwaltung)] > [Data Source (ODBC) (Datenquellen (ODBC))]** .

2 Wechseln Sie im Microsoft ODBC-Datenquellenadministrator zur Registerkarte **[System DSN (System-DSN)]** .

3 Klicken Sie auf **[Add (Hinzufügen)]** und wählen Sie in der angezeigten Liste den geeigneten Oracle-Treiber aus.

Beispiel: **[Oracle in OraHome92]**

4 Klicken Sie auf **[Finish (Fertig stellen)]** .

5 Geben Sie im Dialogfeld **[Oracle ODBC Driver Configuration (Oracle-ODBC-Treiberkonfiguration)]** einen DSN zur Verwendung mit View Composer, eine Beschreibung der Datenquelle sowie eine Benutzer-ID für die Verbindungsherstellung mit der Datenbank ein.

HINWEIS Sie verwenden den DSN bei der Installation des View Composer-Dienstes.

6 Wählen Sie als **[TNS Service Name (TNS-Dienstname)]** den globalen Datenbanknamen im Dropdown-Menü aus.

Der Assistent für die Oracle-Datenbankkonfiguration legt den globalen Datenbanknamen fest.

7 Zum Überprüfen der Datenquelle klicken Sie auf **[Test Connection (Verbindung testen)]** und anschließend auf **[OK]** .

Weiter

Installieren Sie den neuen View Composer-Dienst auf dem vCenter Server-Computer. Siehe „Installieren des View Composer-Dienstes“, auf Seite 38.

Installieren des View Composer-Dienstes

Zur Verwendung von View Composer müssen Sie den View Composer-Dienst auf dem vCenter Server-Computer installieren. View Manager verwendet View Composer zum Erstellen und Bereitstellen von Linked-Clone-Desktops in vCenter Server.

Sie installieren den View Composer-Dienst auf dem Windows Server-Computer, auf dem vCenter Server installiert ist.

Voraussetzungen

- Stellen Sie sicher, dass Ihre Installation die unter „View Composer-Anforderungen“, auf Seite 9 beschriebenen View Composer-Anforderungen erfüllt.
- Stellen Sie sicher, dass Sie über eine Lizenz zur Installation und Verwendung von View Composer verfügen.
- Erstellen Sie in vCenter Server einen Ressourcenpool auf dem ESX-Host oder Cluster, auf dem Sie die Linked-Clone-Desktops speichern möchten.
- Wird auf dem vCenter Server-Computer die Windows-Firewall ausgeführt, müssen Sie sicherstellen, dass der vom View Composer-Dienst zur Kommunikation mit View Connection Server verwendete Port zugänglich ist. Sie können diesen Port zur Ausnahmeliste hinzufügen oder den lokalen Firewall-Dienst deaktivieren. Sie geben diesen Port bei der Installation des View Composer-Dienstes an.
- Stellen Sie sicher, dass Sie über den DSN, den Benutzernamen des Domänenadministrators und das Kennwort verfügen, den/das Sie im ODBC-Datenquellenadministrator angegeben haben. Sie geben diese Informationen bei der Installation des View Composer-Dienstes an.

Vorgehensweise

1 Laden Sie das Installationsprogramm für VMware View Composer von der VMware-Produktseite unter http://www.vmware.com/de/products/ auf den Windows Server-Computer herunter, auf dem vCenter Server installiert ist.

Der Name der Installationsdatei lautet `VMware-viewcomposer-`*`xxxxxx`*`.exe`, wobei *xxxxxx* für die Build-Nummer steht. Diese Installationsdatei installiert den View Composer-Dienst auf 64-Bit- und 32-Bit-Windows Server-Betriebssystemen.

2 Zum Starten des View Composer-Installationsprogramms doppelklicken Sie auf die Installationsdatei.

Auf Windows Server 2008-Computern müssen Sie möglicherweise mit der rechten Maustaste auf die Installationsdatei klicken und **[Run As Administrator (Als Administrator ausführen)]** auswählen.

3 Stimmen Sie den Lizenzbedingungen von VMware zu.

4 Übernehmen oder ändern Sie den Zielordner.

5 Geben Sie den DSN für die View Composer-Datenbank ein, den Sie im ODBC-Datenquellenadministrator für Microsoft oder Oracle eingegeben haben.

Beispiel: **`VMware View Composer`**

HINWEIS Wenn Sie keinen DSN für die View Composer-Datenbank konfiguriert haben, klicken Sie auf **[ODBC DSN Setup (ODBC-DSN-Setup)]** , um jetzt einen Namen zu konfigurieren.

6 Geben Sie den Benutzernamen des Domänenadministrators und das Kennwort ein, den/das Sie im ODBC-Datenquellenadministrator angegeben haben.

7 Geben Sie eine Portnummer ein oder übernehmen Sie den Standardwert.

View Connection Server verwendet diesen Port zur Kommunikation mit dem View Composer-Dienst.

8 Stellen Sie ein SSL-Zertifikat bereit.

Option	Aktion
Create default SSL certificate (SSL-Standardzertifikat erstellen)	Aktivieren Sie diese Optionsschaltfläche, um ein SSL-Standardzertifikat für den View Composer-Dienst zu erstellen.
Use an existing SSL certificate (Vorhandenes SSL-Zertifikat verwenden)	Aktivieren Sie diese Optionsschaltfläche, wenn Sie über ein SSL-Zertifikat verfügen, das Sie für den View Composer-Dienst verwenden möchten. Wählen Sie ein SSL-Zertifikat in der Liste aus.

9 Klicken Sie auf **[Install (Installieren)]** und **[Finish (Fertig stellen)]** , um die Installation des View Composer-Dienstes abzuschließen.

Der VMware View Composer-Dienst wird auf dem vCenter Server-Computer gestartet.

Konfigurieren der Infrastruktur für View Composer

Sie können die Vorteile von Funktionen in vSphere, vCenter Server, Active Directory und anderen Komponenten Ihrer Infrastruktur nutzen, um die Leistung, Verfügbarkeit und Zuverlässigkeit von View Composer zu optimieren.

Konfigurieren der vSphere-Umgebung für View Composer

Zur Unterstützung von View Composer sollten Sie verschiedene empfohlene Vorgehensweisen beachten, wenn Sie vCenter Server, ESX und andere vSphere-Komponenten installieren und konfigurieren.

Die nachfolgend vorgestellten empfohlenen Vorgehensweisen sorgen dafür, dass View Composer in der vSphere-Umgebung optimal ausgeführt wird.

- Nachdem Sie die Pfad- und Ordnerinformationen für virtuelle Linked-Clone-Maschinen angegeben haben, sollten Sie die Informationen nicht in vCenter Server ändern. Verwenden Sie stattdessen View Administrator zum Ändern der Ordnerinformationen.

  Wenn Sie die Informationen in vCenter Server ändern, kann View Manager die virtuellen Maschinen in vCenter Server nicht erfolgreich ermitteln.

- Wenn Sie mehr als 120 virtuelle Maschinen als Linked-Clone-Desktops erstellen, bearbeiten Sie die vSwitch-Einstellungen auf dem ESX-Host, um die Anzahl der Ports für die virtuellen Maschinen zu erhöhen. Standardmäßig ist ESX für 120 Ports konfiguriert.

- Wenn Sie Linked-Clone-Desktop in einem Ressourcenpool bereitstellen, stellen Sie sicher, dass Ihre vSphere-Umgebung über ausreichende CPU- und Arbeitsspeicherressourcen verfügt, um die benötigte Anzahl an Desktops zu hosten. Verwenden Sie vSphere Client zur Überwachung der CPU- und Arbeitsspeichernutzung in Ressourcenpools.

- Ein Cluster kann maximal acht ESX-Hosts enthalten. In einer umfangreichen View Composer-Umgebung müssen Sie möglicherweise zahlreiche Cluster mit jeweils acht Hosts konfigurieren.
- Verwenden Sie vSphere DRS. DRS sorgt für eine effiziente Verteilung der virtuellen Linked-Clone-Maschinen auf Ihre Hosts.

HINWEIS Storage vMotion wird für Linked-Clone-Desktops nicht unterstützt.

Zusätzliche empfohlene Vorgehensweisen für View Composer

Um eine optimale Funktion von View Composer sicherzustellen, sollten Sie sich vergewissern, dass DNS (Dynamic Name Service) ordnungsgemäß arbeitet. Zusätzlich sollten Sie zeitversetzte Prüfungen mithilfe einer Antivirensoftware durchführen.

Indem Sie sicherstellen, dass die DNS-Auflösung ordnungsgemäß funktioniert, können Sie durch DNS-Fehler ausgelöste Probleme beseitigen. Der View Composer-Dienst stützt sich bei der Kommunikation mit anderen Computern auf eine dynamische Namensauflösung. Zum Testen der DNS-Funktion senden Sie ein Ping-Signal an die Active Directory- und View Connection Server-Computer. Verwenden Sie hierbei die Computernamen.

Wenn Sie die Ausführung Ihrer Antivirensoftware zeitversetzt planen, wird die Leistung der Linked-Clone-Desktops nicht beeinträchtigt. Wenn die Antivirensoftware auf allen Linked-Clone-Desktops gleichzeitig ausgeführt wird, treten übermäßige E/A-Vorgänge pro Sekunde in Ihrem Speichersubsystem auf. Diese hohe Aktivität kann sich negativ auf die Leistung der Linked-Clone-Desktops auswirken.

Installieren von View Connection Server 5

Zur Verwendung von View Connection Server installieren Sie die Software auf unterstützten Computern, konfigurieren die erforderlichen Komponenten und nehmen ggf. eine Optimierung der Komponenten vor.

Dieses Kapitel behandelt die folgenden Themen:

- „Installieren der View Connection Server-Software“, auf Seite 41
- „Konfigurieren von Benutzerkonten für vCenter Server und View Composer“, auf Seite 56
- „Anfängliches Konfigurieren von View Connection Server“, auf Seite 60
- „Konfigurieren von View Client-Verbindungen“, auf Seite 64
- „Größeneinstellungen für Windows Server zur Unterstützung Ihrer Bereitstellung“, auf Seite 67

Installieren der View Connection Server-Software

Je nachdem, welche Anforderungen in Bezug auf Leistung, Verfügbarkeit und Sicherheit für Ihre View-Bereitstellung gelten, können Sie eine einzelne Instanz oder replizierte Instanzen von View Connection Server und Sicherheitsserver installieren. Sie müssen mindestens eine Instanz von View Connection Server installieren.

Bei der Installation von View Connection Server wählen Sie die Art der Installation aus.

Standardinstallation	Generiert eine View Connection Server-Instanz mit einer neuen View LDAP-Konfiguration.
Replikatinstallation	Generiert eine View Connection Server-Instanz mit einer View LDAP-Konfiguration, die von einer vorhandenen Instanz kopiert wird.
Sicherheitsserverinstallation	Generiert eine Instanz von View Connection Server, die einen zusätzlichen Sicherheits-Layer zwischen dem Internet und Ihrem internen Netzwerk hinzufügt.

Installationsvoraussetzungen für View Connection Server

Bevor Sie View Connection Server installieren, müssen Sie sicherstellen, dass Ihre Installationsumgebung die geltenden Voraussetzungen erfüllt.

Für View Connection Server ist ein gültiger Lizenzschlüssel für View Manager erforderlich. Die folgenden Lizenzschlüssel sind verfügbar:

- View Manager
- View Manager mit View Composer und lokalem Modus

Sie müssen View Connection Server-Host zu einer Active Directory-Domäne hinzufügen. View Connection Server unterstützt die folgenden Versionen von Active Directory:

- Windows 2000 Active Directory
- Windows 2003 Active Directory
- Windows 2008 Active Directory

Bei dem View Connection Server-Host darf es sich nicht um einen Domänencontroller handeln.

HINWEIS Durch View Connection Server werden keine Aktualisierungen am Active Directory-Schema oder der Active Directory-Konfiguration vorgenommen, und es sind auch keine Aktualisierungen erforderlich.

Installieren Sie View Connection Server nicht auf Systemen, auf denen die Windows Terminal Server-Rolle installiert ist. Sie müssen die Windows Terminal Server-Rolle von einem System entfernen, auf dem Sie View Connection Server installieren möchten.

Installieren Sie View Connection Server nicht auf einem System, das andere Funktionen oder Rollen innehat. Verwenden Sie beispielsweise nicht das System, das Sie zum Hosten von vCenter Server verwenden.

Das System für die Installation von View Connection Server muss über eine statische IP-Adresse verfügen.

Zur Installation von View Connection Server müssen Sie ein Domänenbenutzerkonto mit Administratorberechtigungen für das System verwenden.

Installieren von View Connection Server mit einer neuen Konfiguration

Um View Connection Server als einen einzelnen Server oder als erste Instanz in einer Gruppe replizierter View Connection Server-Instanzen zu installieren, verwenden Sie die Standardinstallationsoption.

Wenn Sie die Standardinstallationsoption wählen, wird bei der Installation eine neue, lokale View LDAP-Konfiguration erstellt. Die Installation lädt Schemadefinitionen, DIT-Definition (Directory Information Tree) und ACLs und initialisiert die Daten.

Nach der Installation verwalten Sie die meisten View LDAP-Konfigurationsdaten mithilfe von View Administrator. View Connection Server verwaltet einige View LDAP-Einträge automatisch.

Voraussetzungen

- Stellen Sie sicher, dass Sie sich als Domänenbenutzer mit Administratorberechtigungen auf dem Windows Server-Computer anmelden können, auf dem Sie View Connection Server installieren.
- Stellen Sie sicher, dass Ihre Installation die unter „View Connection Server-Anforderungen“, auf Seite 7 beschriebenen Anforderungen erfüllt.
- Bereiten Sie Ihre Umgebung für die Installation vor. Siehe „Installationsvoraussetzungen für View Connection Server“, auf Seite 41.
- Machen Sie sich mit den eingehenden TCP-Ports vertraut, die in der Windows-Firewall für die View Connection Server-Instanzen geöffnet werden müssen. Siehe „Firewall-Regeln für View Connection Server“, auf Seite 45.

Vorgehensweise

1 Laden Sie das Installationsprogramm für View Connection Server von der VMware-Produktseite unter http://www.vmware.com/de/products/ auf den Windows Server-Computer herunter.

   Der Name der Installationsdatei lautet `VMware-viewconnectionserver-4.5.x-xxxxxx.exe` oder `VMware-viewconnectionserver-x86_64-4.5.x-xxxxxx.exe`, wobei *xxxxxx* für die Build-Nummer steht.

2 Zum Starten des View Connection Server-Installationsprogramms doppelklicken Sie auf die Installationsdatei.

3 Stimmen Sie den Lizenzbedingungen von VMware zu.

4 Übernehmen oder ändern Sie den Zielordner.

5 Wählen Sie die Installationsoption **[View Standard Server]** .

6 Akzeptieren Sie den Microsoft-Softwarezusatzlizenzvertrag für Microsoft Active Directory Application Mode (ADAM).

7 Wenn Sie View Connection Server unter Windows Server 2008 installieren, wählen Sie aus, wie der Windows-Firewall-Dienst konfiguriert werden soll.

Option	Aktion
Configure Windows Firewall automatically (Windows-Firewall automatisch konfigurieren)	Lassen Sie die Windows-Firewall durch das Installationsprogramm so konfigurieren, dass die erforderlichen eingehenden TCP-Protokollverbindungen zugelassen werden.
Do not configure Windows Firewall (Windows-Firewall nicht konfigurieren)	Konfigurieren Sie die Firewall-Regeln für Windows manuell.

   Wenn Sie View Connection Server unter Windows Server 2003 installieren, müssen Sie die erforderlichen Firewall-Regeln für Windows manuell konfigurieren.

8 Schließen Sie die Installation von View Connection Server mit dem Installations-Assistenten ab.

Die VMware View-Dienste werden auf dem Windows Server-Computer installiert:

- VMware View Connection Server
- VMware View-Framework-Komponente
- VMware View-Nachrichtenbuskomponente
- VMware View-Skripthost
- VMware View-Sicherheits-Gateway-Komponente
- VMware View-Webkomponente
- VMware VDMDS, zur Bereitstellung der View LDAP-Verzeichnisdienste

Informationen zu diesen Diensten finden Sie im *VMware View-Administratorhandbuch*.

Weiter

Führen Sie eine anfängliche Konfiguration von View Connection Server durch.

Wenn Sie replizierte View Connection Server-Instanzen und Sicherheitsserver in Ihrer Bereitstellung nutzen möchten, müssen Sie jede Serverinstanz durch Ausführung der View Connection Server-Installationsdatei installieren.

Wenn Sie View Connection Server erneut unter einem Windows Server 2008-Betriebssystem installieren und einen Datenerfassungs-Set zur Überwachung der Leistungsdaten konfiguriert haben, stoppen Sie den Datenerfassungs-Set und starten Sie ihn erneut.

Unbeaufsichtigte Installation von View Connection Server

Sie können die Microsoft Windows Installer-Funktion (MSI) für die unbeaufsichtigte Installation dazu verwenden, eine Standardinstallation von View Connection Server auf mehreren Windows-Computern durchzuführen. Bei einer unbeaufsichtigten Installation verwenden Sie die Befehlszeile und müssen nicht auf Eingabeaufforderungen des Assistenten reagieren.

Die unbeaufsichtigte Installation ermöglicht eine effiziente Bereitstellung von View-Komponenten in einem großen Unternehmen.

Voraussetzungen

- Stellen Sie sicher, dass Sie sich als Domänenbenutzer mit Administratorberechtigungen auf dem Windows Server-Computer anmelden können, auf dem Sie View Connection Server installieren.
- Stellen Sie sicher, dass Ihre Installation die unter „View Connection Server-Anforderungen“, auf Seite 7 beschriebenen Anforderungen erfüllt.
- Bereiten Sie Ihre Umgebung für die Installation vor. Siehe „Installationsvoraussetzungen für View Connection Server“, auf Seite 41.
- Stellen Sie sicher, dass der Windows-Computer, auf dem Sie View Connection Server installieren, über Version 2.0 oder eine höhere Version des MSI-Laufzeitmoduls verfügt. Weitere Informationen finden Sie auf der Microsoft-Website.
- Machen Sie sich mit den MSI-Befehlszeilenoptionen vertraut. Siehe „Microsoft Windows Installer-Befehlszeilenoptionen“, auf Seite 54.
- Machen Sie sich mit den verfügbaren Eigenschaften für die unbeaufsichtigte Installation einer Standardinstallation von View Connection Server vertraut. Siehe „Eigenschaften für die unbeaufsichtigte Installation einer View Connection Server-Standardinstallation“, auf Seite 45.

Vorgehensweise

1 Laden Sie das Installationsprogramm für View Connection Server von der VMware-Produktseite unter http://www.vmware.com/de/products/ auf den Windows Server-Computer herunter.

   Der Name der Installationsdatei lautet `VMware-viewconnectionserver-4.5.`*`x-xxxxxx`*`.exe` oder `VMware-viewconnectionserver-x86_64-4.5.`*`x-xxxxxx`*`.exe`, wobei *xxxxxx* für die Build-Nummer steht.

2 Öffnen Sie auf dem Windows Server-Computer eine Eingabeaufforderung.

3 Geben Sie den Installationsbefehl in einer Zeile ein.

   Beispiel: `VMware-viewconnectionserver-4.5.`*`x-xxxxxx`*`.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=1"`

Die VMware View-Dienste werden auf dem Windows Server-Computer installiert. Weitere Informationen finden Sie unter „Installieren von View Connection Server mit einer neuen Konfiguration“, auf Seite 42.

Eigenschaften für die unbeaufsichtigte Installation einer View Connection Server-Standardinstallation

Sie können spezielle Eigenschaften einschließen, wenn Sie eine unbeaufsichtigte Installation einer View Connection Server-Standardinstallation über die Befehlszeile ausführen. Sie müssen hierbei das Format *EIGENSCHAFT=Wert* einhalten, damit Microsoft Windows Installer (MSI) die Eigenschaften und Werte interpretieren kann.

Tabelle 5-1. MSI-Eigenschaften für die unbeaufsichtigte Installation von View Connection Server in einer Standardinstallation

MSI-Eigenschaft	Beschreibung	Standardwert
INSTALLDIR	Der Pfad und der Ordner, in dem die View Connection Server-Software installiert wird. Beispiel: `INSTALLDIR=""D:\abc\Mein Ordner""` Die zweifach gesetzten doppelten Anführungszeichen um den Pfad sorgen dafür, dass das MSI-Installationsprogramm das Leerzeichen im Pfad ignoriert.	`%ProgramFiles%\VMware, Inc.\VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	Die Art der View Connection Server-Installation: ■ **1**. Standardinstallation ■ **2**. Replikatinstallation ■ **3**. Sicherheitsserverinstallation ■ **4**. View Transfer Server-Installation Für eine Standardinstallation definieren Sie `VDM_SERVER_INSTANCE_TYPE=1`	1
FWCHOICE	Diese MSI-Eigenschaft legt fest, ob eine Firewall für die View Connection Server-Instanz konfiguriert werden soll. Mit dem Wert 1 wird eine Firewall festgelegt. Mit dem Wert 2 wird keine Firewall festgelegt. Beispiel: `FWCHOICE=1`	1

Firewall-Regeln für View Connection Server

Bestimmte eingehende TCP-Ports müssen an der Firewall für View Connection Server-Instanzen und Sicherheitsserver geöffnet werden.

Wenn Sie View Connection Server auf Windows Server 2008 installieren, kann das Installationsprogramm die erforderlichen Regeln für die Windows-Firewall optional für Sie konfigurieren.

Wenn Sie View Connection Server auf Windows Server 2003 installieren, müssen Sie die erforderlichen Firewall-Regeln für Windows manuell konfigurieren.

Tabelle 5-2 listet die eingehenden TCP-Ports auf, die an der Firewall für View Connection Server-Instanzen und Sicherheitsserver geöffnet werden müssen.

Tabelle 5-2. TCP-Ports für View Connection Server-Instanzen

Protokoll	Ports	Typ der View Connection Server-Instanz
JMS	4001	Standard- und Replikatserver
JMSIR	4100	Standard- und Replikatserver
AJP13	8009	Standard- und Replikatserver
HTTP	80	Standard-, Replikat- und Sicherheitsserver
HTTPS	443	Standard-, Replikat- und Sicherheitsserver

Installieren einer replizierten Instanz von View Connection Server

Zur Bereitstellung von hoher Verfügbarkeit und Lastausgleich können Sie eine oder mehrere zusätzliche Instanzen von View Connection Server installieren, die eine vorhandene View Connection Server-Instanz replizieren. Nach einer Replikatinstallation sind die vorhandene und neu installierte Instanzen von View Connection Server identisch.

Wenn Sie eine replizierte Instanz installieren, kopiert View Manager die View LDAP-Konfigurationsdaten von der vorhandenen View Connection Server-Instanz.

Nach der Installation verwaltet die View Manager-Software identische View LDAP-Konfigurationsdaten auf allen View Connection Server-Instanzen in der replizierten Gruppe. Werden an einer Instanz Änderungen vorgenommen, werden die aktualisierten Informationen auf die weiteren Instanzen kopiert.

Fällt eine replizierte Instanz aus, setzen die weiteren Instanzen in der Gruppe ihren Betrieb fort. Sobald die ausgefallene Instanz ihren Betrieb wieder aufnimmt, wird ihre Konfiguration mit den Änderungen aktualisieren, die während des Ausfalls durchgeführt wurden.

Hinweis Diese Replikationsfunktionalität wird über View LDAP bereitgestellt, das dieselbe Replikationstechnologie verwendet wie Active Directory.

Voraussetzungen

- Stellen Sie sicher, dass mindestens eine View Connection Server-Instanz im Netzwerk installiert und konfiguriert wurde.
- Stellen Sie sicher, dass Sie sich als Domänenbenutzer mit Administratorberechtigungen auf dem Windows Server-Computer anmelden können, auf dem Sie die replizierte Instanz installieren möchten.
- Wenn sich die vorhandene View Connection Server-Instanz in einer anderen Domäne befindet als die replizierte Instanz, muss der Domänenbenutzer zusätzlich über lokale Administratorberechtigungen auf dem Windows Server-Computer verfügen, auf dem die vorhandene Instanz installiert ist.
- Stellen Sie sicher, dass Ihre Installation die unter „View Connection Server-Anforderungen“, auf Seite 7 beschriebenen Anforderungen erfüllt.
- Stellen Sie sicher, dass die Computer, auf denen Sie replizierte View Connection Server-Instanzen installieren, über ein Hochleistungs-LAN miteinander verbunden sind. Siehe „Netzwerkanforderungen für replizierte View Connection Server-Instanzen“, auf Seite 9.
- Bereiten Sie Ihre Umgebung für die Installation vor. Siehe „Installationsvoraussetzungen für View Connection Server“, auf Seite 41.
- Machen Sie sich mit den eingehenden TCP-Ports vertraut, die in der Windows-Firewall für die View Connection Server-Instanzen geöffnet werden müssen. Siehe „Firewall-Regeln für View Connection Server“, auf Seite 45.

Vorgehensweise

1 Laden Sie das Installationsprogramm für View Connection Server von der VMware-Produktseite unter http://www.vmware.com/de/products/ auf den Windows Server-Computer herunter.

   Der Name der Installationsdatei lautet `VMware-viewconnectionserver-4.5.x-xxxxxx.exe` oder `VMware-viewconnectionserver-x86_64-4.5.x-xxxxxx.exe`, wobei *xxxxxx* für die Build-Nummer steht.

2 Zum Starten des View Connection Server-Installationsprogramms doppelklicken Sie auf die Installationsdatei.

3 Stimmen Sie den Lizenzbedingungen von VMware zu.

4 Übernehmen oder ändern Sie den Zielordner.

5 Wählen Sie die Installationsoption **[View Replica Server]** .

6 Geben Sie den Hostnamen oder die IP-Adresse der vorhandenen View Connection Server-Instanz ein, die Sie replizieren möchten.

7 Akzeptieren Sie den Microsoft-Softwarezusatzlizenzvertrag für Microsoft Active Directory Application Mode (ADAM).

8 Wenn Sie View Connection Server unter Windows Server 2008 installieren, wählen Sie aus, wie der Windows-Firewall-Dienst konfiguriert werden soll.

Option	Aktion
Configure Windows Firewall automatically (Windows-Firewall automatisch konfigurieren)	Lassen Sie die Windows-Firewall durch das Installationsprogramm so konfigurieren, dass die erforderlichen eingehenden TCP-Protokollverbindungen zugelassen werden.
Do not configure Windows Firewall (Windows-Firewall nicht konfigurieren)	Konfigurieren Sie die Firewall-Regeln für Windows manuell.

   Wenn Sie View Connection Server unter Windows Server 2003 installieren, müssen Sie die erforderlichen Firewall-Regeln für Windows manuell konfigurieren.

9 Schließen Sie die Installation der replizierten Instanz mit dem Installations-Assistenten ab.

Die VMware View-Dienste werden auf dem Windows Server-Computer installiert:

- VMware View Connection Server
- VMware View-Framework-Komponente
- VMware View-Nachrichtenbuskomponente
- VMware View-Skripthost
- VMware View-Sicherheits-Gateway-Komponente
- VMware View-Webkomponente
- VMware VDMDS, zur Bereitstellung der View LDAP-Verzeichnisdienste

Informationen zu diesen Diensten finden Sie im *VMware View-Administratorhandbuch*.

Weiter

Eine replizierte Instanz von View Connection Server erfordert keine anfängliche Konfiguration. Die replizierte Instanz erbt ihre Konfiguration von der vorhandenen View Connection Server-Instanz.

Wenn Sie View Connection Server erneut unter einem Windows Server 2008-Betriebssystem installieren und einen Datenerfassungs-Set zur Überwachung der Leistungsdaten konfiguriert haben, stoppen Sie den Datenerfassungs-Set und starten Sie ihn erneut.

Wiederholen Sie diese Vorgehensweise, um zusätzliche replizierte Instanzen zu installieren.

Unbeaufsichtigte Installation einer replizierten Instanz von View Connection Server

Sie können die Microsoft Windows Installer-Funktion (MSI) für die unbeaufsichtigte Installation dazu verwenden, eine replizierte Instanz von View Connection Server auf mehreren Windows-Computern zu installieren. Bei einer unbeaufsichtigten Installation verwenden Sie die Befehlszeile und müssen nicht auf Eingabeaufforderungen des Assistenten reagieren.

Die unbeaufsichtigte Installation ermöglicht eine effiziente Bereitstellung von View-Komponenten in einem großen Unternehmen.

Voraussetzungen

- Stellen Sie sicher, dass mindestens eine View Connection Server-Instanz im Netzwerk installiert und konfiguriert wurde.
- Stellen Sie sicher, dass Sie sich als Domänenbenutzer mit Administratorberechtigungen auf dem Windows Server-Computer anmelden können, auf dem Sie die replizierte Instanz installieren möchten.
- Wenn sich die vorhandene View Connection Server-Instanz in einer anderen Domäne befindet als die replizierte Instanz, muss der Domänenbenutzer zusätzlich über lokale Administratorberechtigungen auf dem Windows Server-Computer verfügen, auf dem die vorhandene Instanz installiert ist.
- Stellen Sie sicher, dass Ihre Installation die unter „View Connection Server-Anforderungen“, auf Seite 7 beschriebenen Anforderungen erfüllt.
- Stellen Sie sicher, dass die Computer, auf denen Sie replizierte View Connection Server-Instanzen installieren, über ein Hochleistungs-LAN miteinander verbunden sind. Siehe „Netzwerkanforderungen für replizierte View Connection Server-Instanzen“, auf Seite 9.
- Bereiten Sie Ihre Umgebung für die Installation vor. Siehe „Installationsvoraussetzungen für View Connection Server“, auf Seite 41.
- Machen Sie sich mit den MSI-Befehlszeilenoptionen vertraut. Siehe „Microsoft Windows Installer-Befehlszeilenoptionen“, auf Seite 54.
- Machen Sie sich mit den verfügbaren Eigenschaften für die unbeaufsichtigte Installation einer replizierten Instanz von View Connection Server vertraut. Siehe „Eigenschaften für die unbeaufsichtigte Installation einer replizierten Instanz von View Connection Server“, auf Seite 49.

Vorgehensweise

1 Laden Sie das Installationsprogramm für View Connection Server von der VMware-Produktseite unter http://www.vmware.com/de/products/ auf den Windows Server-Computer herunter.

   Der Name der Installationsdatei lautet `VMware-viewconnectionserver-4.5.`*`x`*`-`*`xxxxxx`*`.exe` oder `VMware-viewconnectionserver-x86_64-4.5.`*`x`*`-`*`xxxxxx`*`.exe`, wobei *xxxxxx* für die Build-Nummer steht.

2 Öffnen Sie auf dem Windows Server-Computer eine Eingabeaufforderung.

3 Geben Sie den Installationsbefehl in einer Zeile ein.

   Beispiel: `VMware-viewconnectionserver-4.5.`*`x`*`-`*`xxxxxx`*`.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=2 ADAM_PRIMARY_NAME=cs1.companydomain.com"`

Die VMware View-Dienste werden auf dem Windows Server-Computer installiert. Weitere Informationen finden Sie unter „Installieren einer replizierten Instanz von View Connection Server“, auf Seite 46.

Eigenschaften für die unbeaufsichtigte Installation einer replizierten Instanz von View Connection Server

Sie können spezielle Eigenschaften einschließen, wenn Sie eine unbeaufsichtigte Installation einer replizierten Instanz von View Connection Server über die Befehlszeile ausführen. Sie müssen hierbei das Format *EIGENSCHAFT=Wert* einhalten, damit Microsoft Windows Installer (MSI) die Eigenschaften und Werte interpretieren kann.

Tabelle 5-3. MSI-Eigenschaften für die unbeaufsichtigte Installation einer replizierten Instanz von View Connection Server

MSI-Eigenschaft	Beschreibung	Standardwert
INSTALLDIR	Der Pfad und der Ordner, in dem die View Connection Server-Software installiert wird. Beispiel: `INSTALLDIR=""D:\abc\Mein Ordner""` Die zweifach gesetzten doppelten Anführungszeichen um den Pfad sorgen dafür, dass das MSI-Installationsprogramm das Leerzeichen im Pfad ignoriert. Diese MSI-Eigenschaft ist optional.	`%ProgramFiles% \VMware, Inc. \VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	Die Art der View Connection Server-Installation: ■ **1**. Standardinstallation ■ **2**. Replikatinstallation ■ **3**. Sicherheitsserverinstallation ■ **4**. View Transfer Server-Installation Für die Installation einer replizierten Instanz verwenden Sie `VDM_SERVER_INSTANCE_TYPE=2` Diese MSI-Eigenschaft ist für eine Standardinstallation optional. Für alle anderen Installationsarten ist die Eigenschaft erforderlich.	1
ADAM_PRIMARY_NAME	Der Hostname oder die IP-Adresse der vorhandenen View Connection Server-Instanz, die Sie replizieren möchten. Beispiel: `ADAM_PRIMARY_NAME=cs1.companydomain.com` Diese MSI-Eigenschaft ist erforderlich.	–
ADAM_PRIMARY_PORT	Der View LDAP-Port der vorhandenen View Connection Server-Instanz, die Sie replizieren. Beispiel: `ADAM_PRIMARY_PORT=cs1.companydomain.com` Diese MSI-Eigenschaft ist optional.	–
FWCHOICE	Diese MSI-Eigenschaft legt fest, ob eine Firewall für die View Connection Server-Instanz konfiguriert werden soll. Mit dem Wert 1 wird eine Firewall festgelegt. Mit dem Wert 2 wird keine Firewall festgelegt. Beispiel: `FWCHOICE=1` Diese MSI-Eigenschaft ist optional.	1

Konfigurieren eines Kennworts für die Paarbildung mit einem Sicherheitsserver

Bevor Sie einen Sicherheitsserver installieren können, müssen Sie ein Kennwort für die Paarbildung mit dem Sicherheitsserver konfigurieren. Das View Connection Server-Installationsprogramm fordert dieses Kennwort während der Installation an.

Das Kennwort für die Paarbildung mit dem Sicherheitsserver ist ein einmaliges Kennwort, das einem Sicherheitsserver die Paarbildung mit einer View Connection Server-Instanz ermöglicht. Das Kennwort läuft ab, nachdem Sie es im View Connection Server-Installationsprogramm angegeben haben.

Vorgehensweise

1 Wählen Sie in View Administrator **[View Configuration (Konfiguration anzeigen)]** > **[Servers (Server)]** .

2 Wählen Sie im Fenster **[View Servers (Server anzeigen)]** die View Connection Server-Instanz, die mit dem Sicherheitsserver kombiniert werden soll.

3 Wählen Sie im Dropdown-Menü **[More Commands (Weitere Befehle)]** die Einstellung **[Specify Security Server Pairing Password (Kennwort für Security Server-Kombination angeben)]** .

4 Geben Sie das Kennwort in den Textfeldern **[Pairing password (Kennwort für Paarbildung)]** und **[Confirm password (Kennwort bestätigen)]** ein und geben Sie einen Zeitüberschreitungswert für das Kennwort ein.

   Sie müssen das Kennwort innerhalb der angegebenen Zeitspanne verwenden.

5 Klicken Sie auf **[OK]** , um das Kennwort zu konfigurieren.

Weiter

Installieren Sie einen Sicherheitsserver. Siehe „Installieren eines Sicherheitsservers“, auf Seite 50.

WICHTIG Wenn Sie das Kennwort für die Paarbildung mit dem Sicherheitsserver nicht innerhalb des angegebenen Zeitraums im View Connection Server-Installationsprogramm angeben, wird das Kennwort ungültig und Sie müssen ein neues Kennwort konfigurieren.

Installieren eines Sicherheitsservers

Ein Sicherheitsserver ist eine Instanz von View Connection Server, die einen zusätzlichen Sicherheits-Layer zwischen dem Internet und Ihrem internen Netzwerk hinzufügt. Sie können einen oder mehrere Sicherheitsserver installieren, die mit einer View Connection Server-Instanz verbunden werden.

Voraussetzungen

- Informationen zu den Anforderungen in Bezug auf Installation und Bereitstellung eines Sicherheitsservers finden Sie im *Planungshandbuch für die VMware View-Architektur*.
- Stellen Sie sicher, dass Ihre Installation die unter „View Connection Server-Anforderungen“, auf Seite 7 beschriebenen Anforderungen erfüllt.
- Bereiten Sie Ihre Umgebung für die Installation vor. Siehe „Installationsvoraussetzungen für View Connection Server“, auf Seite 41.
- Stellen Sie sicher, dass die zur Kombination mit dem Sicherheitsserver vorgesehene View Connection Server-Instanz installiert und konfiguriert wurde und View Connection Server 4.5 ausführt. Sie können einen Sicherheitsserver nicht mit einer älteren Version von View Connection Server kombinieren.
- Stellen Sie sicher, dass die zur Kombination mit dem Sicherheitsserver vorgesehene View Connection Server-Instanz für den Computer zugänglich ist, auf dem Sie den Sicherheitsserver installieren möchten.
- Konfigurieren Sie ein Kennwort für die Paarbildung mit dem Sicherheitsserver. Siehe „Konfigurieren eines Kennworts für die Paarbildung mit einem Sicherheitsserver“, auf Seite 49.
- Machen Sie sich mit dem Format externer URLs vertraut. Siehe „Konfigurieren externer URLs für Tunnelverbindungen“, auf Seite 65.
- Stellen Sie sicher, dass Sie sich als Domänenbenutzer mit lokalen Administratorberechtigungen auf dem Windows Server-Computer anmelden können, auf dem Sie den Sicherheitsserver installieren möchten.
- Machen Sie sich mit den eingehenden TCP-Ports vertraut, die in der Windows-Firewall für einen Sicherheitsserver geöffnet werden müssen. Siehe „Firewall-Regeln für View Connection Server“, auf Seite 45.

Vorgehensweise

1 Laden Sie das Installationsprogramm für View Connection Server von der VMware-Produktseite unter http://www.vmware.com/de/products/ auf den Windows Server-Computer herunter.

Der Name der Installationsdatei lautet `VMware-viewconnectionserver-4.5.x-xxxxxx.exe` oder `VMware-viewconnectionserver-x86_64-4.5.x-xxxxxx.exe`, wobei *xxxxxx* für die Build-Nummer steht.

2 Zum Starten des View Connection Server-Installationsprogramms doppelklicken Sie auf die Installationsdatei.

3 Stimmen Sie den Lizenzbedingungen von VMware zu.

4 Übernehmen oder ändern Sie den Zielordner.

5 Wählen Sie die Installationsoption **[View Security Server]** .

6 Geben Sie den vollqualifizierten Domänennamen oder die IP-Adresse der für die Paarbildung mit dem Sicherheitsserver vorgesehenen View Connection Server-Instanz im Textfeld **[Server]** ein.

Der Sicherheitsserver leitet den Netzwerkdatenverkehr an diese View Connection Server-Instanz weiter.

7 Geben Sie das Kennwort für die Paarbildung mit dem Sicherheitsserver in das Textfeld „Password (Kennwort)“ ein.

Wenn das Kennwort abgelaufen ist, können Sie mit View Administrator ein neues Kennwort konfigurieren und das neue Kennwort im Installationsprogramm angeben.

8 Geben Sie im Textfeld **[External URL (Externe URL)]** die externe URL ein.

Die URL muss das Protokoll, den extern auflösbaren Namen des Sicherheitsservers und die Portnummer enthalten. Tunnelclients, die außerhalb Ihres Netzwerks ausgeführt werden, verwenden diese URL zur Verbindungsherstellung mit dem Sicherheitsserver.

Beispiel: `https://view.example.com:443`

9 Wenn Sie den Sicherheitsserver unter Windows Server 2008 installieren, wählen Sie aus, wie der Windows-Firewall-Dienst konfiguriert werden soll.

Option	Aktion
Configure Windows Firewall automatically (Windows-Firewall automatisch konfigurieren)	Lassen Sie die Windows-Firewall durch das Installationsprogramm so konfigurieren, dass die erforderlichen eingehenden TCP-Protokollverbindungen zugelassen werden.
Do not configure Windows Firewall (Windows-Firewall nicht konfigurieren)	Konfigurieren Sie die Firewall-Regeln für Windows manuell.

Wenn Sie den Sicherheitsserver unter Windows Server 2003 installieren, müssen Sie die erforderlichen Firewall-Regeln für Windows manuell konfigurieren.

10 Schließen Sie die Installation des Sicherheitsservers mit dem Installations-Assistenten ab.

Die Dienste für den Sicherheitsserver werden auf dem Windows Server-Computer installiert:

- VMware View Security Server
- VMware View-Framework-Komponente
- VMware View-Sicherheits-Gateway-Komponente

Informationen zu diesen Diensten finden Sie im *VMware View-Administratorhandbuch*.

Der Sicherheitsserver erscheint im Fensterbereich **[Security Servers (Sicherheitsserver)]** von View Administrator.

Weiter

Wenn Sie den Sicherheitsserver erneut unter einem Windows Server 2008-Betriebssystem installieren und einen Datenerfassungs-Set zur Überwachung der Leistungsdaten konfiguriert haben, stoppen Sie den Datenerfassungs-Set und starten Sie ihn erneut.

Unbeaufsichtigte Installation eines Sicherheitsservers

Sie können die Microsoft Windows Installer-Funktion (MSI) für die unbeaufsichtigte Installation dazu verwenden, einen Sicherheitsserver auf mehreren Windows-Computern zu installieren. Bei einer unbeaufsichtigten Installation verwenden Sie die Befehlszeile und müssen nicht auf Eingabeaufforderungen des Assistenten reagieren.

Die unbeaufsichtigte Installation ermöglicht eine effiziente Bereitstellung von View-Komponenten in einem großen Unternehmen.

Voraussetzungen

- Informationen zu den Anforderungen in Bezug auf Installation und Bereitstellung eines Sicherheitsservers finden Sie im *Planungshandbuch für die VMware View-Architektur*.
- Stellen Sie sicher, dass Ihre Installation die unter „View Connection Server-Anforderungen“, auf Seite 7 beschriebenen Anforderungen erfüllt.
- Bereiten Sie Ihre Umgebung für die Installation vor. Siehe „Installationsvoraussetzungen für View Connection Server“, auf Seite 41.
- Stellen Sie sicher, dass die zur Kombination mit dem Sicherheitsserver vorgesehene View Connection Server-Instanz installiert und konfiguriert wurde und View Connection Server 4.5 ausführt. Sie können einen Sicherheitsserver nicht mit einer älteren Version von View Connection Server kombinieren.
- Konfigurieren Sie ein Kennwort für die Paarbildung mit dem Sicherheitsserver. Siehe „Konfigurieren eines Kennworts für die Paarbildung mit einem Sicherheitsserver“, auf Seite 49.
- Machen Sie sich mit dem Format externer URLs vertraut. Siehe „Konfigurieren externer URLs für Tunnelverbindungen“, auf Seite 65.
- Stellen Sie sicher, dass Sie sich als Domänenbenutzer mit lokalen Administratorberechtigungen auf dem Windows Server-Computer anmelden können, auf dem Sie den Sicherheitsserver installieren möchten.
- Machen Sie sich mit den MSI-Befehlszeilenoptionen vertraut. Siehe „Microsoft Windows Installer-Befehlszeilenoptionen“, auf Seite 54.
- Machen Sie sich mit den verfügbaren Eigenschaften für die unbeaufsichtigte Installation eines Sicherheitsservers vertraut. Siehe „Eigenschaften für die unbeaufsichtigte Installation eines Sicherheitsservers“, auf Seite 53.

Vorgehensweise

1 Laden Sie das Installationsprogramm für View Connection Server von der VMware-Produktseite unter http://www.vmware.com/de/products/ auf den Windows Server-Computer herunter.

   Der Name der Installationsdatei lautet `VMware-viewconnectionserver-4.5.`*`x-xxxxxx`*`.exe` oder `VMware-viewconnectionserver-x86_64-4.5.`*`x-xxxxxx`*`.exe`, wobei *xxxxxx* für die Build-Nummer steht.

2 Öffnen Sie auf dem Windows Server-Computer eine Eingabeaufforderung.

3 Geben Sie den Installationsbefehl in einer Zeile ein.

   Beispiel: `VMware-viewconnectionserver-4.5.`*`x-xxxxxx`*`.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=3 VDM_SERVER_NAME=cs1.companydomain.com VDM_SERVER_SS_EXTURL=https://ss1.companydomain.com:443 VDM_SERVER_SS_PWD=secret"`

Die VMware View-Dienste werden auf dem Windows Server-Computer installiert. Weitere Informationen finden Sie unter „Installieren eines Sicherheitsservers“, auf Seite 50.

Eigenschaften für die unbeaufsichtigte Installation eines Sicherheitsservers

Sie können spezielle Eigenschaften einschließen, wenn Sie eine unbeaufsichtigte Installation eines Sicherheitsservers über die Befehlszeile ausführen. Sie müssen hierbei das Format *EIGENSCHAFT=Wert* einhalten, damit Microsoft Windows Installer (MSI) die Eigenschaften und Werte interpretieren kann.

Tabelle 5-4. MSI-Eigenschaften für die unbeaufsichtigte Installation eines Sicherheitsservers

MSI-Eigenschaft	Beschreibung	Standardwert
INSTALLDIR	Der Pfad und der Ordner, in dem die View Connection Server-Software installiert wird. Beispiel: `INSTALLDIR=""D:\abc\Mein Ordner""` Die zweifach gesetzten doppelten Anführungszeichen um den Pfad sorgen dafür, dass das MSI-Installationsprogramm das Leerzeichen im Pfad ignoriert. Diese MSI-Eigenschaft ist optional.	`%ProgramFiles% \VMware, Inc. \VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	Die Art der View Connection Server-Installation: ■ **1**. Standardinstallation ■ **2**. Replikatinstallation ■ **3**. Sicherheitsserverinstallation ■ **4**. View Transfer Server-Installation Für die Installation eines Sicherheitsservers verwenden Sie `VDM_SERVER_INSTANCE_TYPE=3` Diese MSI-Eigenschaft ist für eine Standardinstallation optional. Für alle anderen Installationsarten ist die Eigenschaft erforderlich.	1
VDM_SERVER_NAME	Der Hostname oder die IP-Adresse der vorhandenen View Connection Server-Instanz, die ein Paar mit dem Sicherheitsserver bildet. Beispiel: `VDM_SERVER_NAME=cs1.companydomain.com` Diese MSI-Eigenschaft ist erforderlich.	–
VDM_SERVER_SS_EXTURL	Die externe URL des Sicherheitsservers. Die URL muss das Protokoll, den extern auflösbaren Namen des Sicherheitsservers und die Portnummer enthalten. Beispiel: `VDM_SERVER_SS_EXTURL=https://ss1.companydomain.com:443` Diese MSI-Eigenschaft ist erforderlich.	–
VDM_SERVER_SS_PWD	Das Kennwort für die Paarbildung mit dem Sicherheitsserver. Beispiel: `VDM_SERVER_SS_PWD=secret` Diese MSI-Eigenschaft ist erforderlich.	–
FWCHOICE	Diese MSI-Eigenschaft legt fest, ob eine Firewall für die View Connection Server-Instanz konfiguriert werden soll. Mit dem Wert 1 wird eine Firewall festgelegt. Mit dem Wert 2 wird keine Firewall festgelegt. Beispiel: `FWCHOICE=1` Diese MSI-Eigenschaft ist optional.	1

Microsoft Windows Installer-Befehlszeilenoptionen

Zur unbeaufsichtigten Installation von View-Komponenten müssen Sie die Befehlszeilenoptionen und Eigenschaften von Microsoft Windows Installer (MSI) verwenden. Die Installationsprogramme für View-Komponenten sind MSI-Programme und verwenden standardmäßige MSI-Funktionen. Sie können auch MSI-Befehlszeilenoptionen zum unbeaufsichtigten Deinstallieren von View-Komponenten verwenden.

Weitere Informationen zum Microsoft Windows Installer (MSI) finden Sie auf der Microsoft-Website. Informationen zu MSI-Befehlszeilenoptionen erhalten Sie, wenn Sie auf der Microsoft Developer Network (MSDN) Library-Website nach MSI-Befehlszeilenoptionen suchen. Informationen zur Verwendung der MSI-Befehlszeile erhalten Sie, indem Sie auf dem Computer mit der View-Komponente eine Eingabeaufforderung öffnen und `msiexec /?` eingeben.

Für die unbeaufsichtigte Installation einer View-Komponente deaktivieren Sie zunächst das Bootstrap-Programm, mit dem das Installationsprogramm in ein temporäres Verzeichnis extrahiert und eine interaktive Installation gestartet wird.

Tabelle 5-5 zeigt die Befehlszeilenoptionen, die das Bootstrap-Programm des Installationsprogramms steuern.

Tabelle 5-5. Befehlszeilenoptionen für das Bootstrap-Programm einer View-Komponente

Option	Beschreibung
`/s`	Deaktiviert den Bootstrap-Begrüßungsbildschirm und das Dialogfeld für das Extrahieren, sodass keine interaktiven Dialogfenster angezeigt werden. Beispiel: `VMware-viewconnectionserver-4.5.`*`x-xxxxxx`*`.exe /s` Die Option `/s` ist erforderlich, um eine unbeaufsichtigte Installation auszuführen.
`/v"` *`MSI-Befehlszeilenoptionen`*`"`	Weist das Installationsprogramm an, die in doppelte Anführungszeichen eingeschlossene Zeichenfolge, die an der Befehlszeile eingegeben wurde, als MSI-Optionssatz auszuwerten. Sie müssen die Befehlszeileneinträge in doppelte Anführungszeichen einschließen. Platzieren Sie ein doppeltes Anführungszeichen nach `/v` und am Ende der Befehlszeile. Beispiel: `VMware-viewagent-4.5.`*`x-xxxxxx`*`.exe /s /v"`*`Befehlszeilenoptionen`*`"` Damit das MSI-Installationsprogramm eine Zeichenfolge mit Leerzeichen richtig auswertet, müssen Sie die Zeichenfolge in zwei Sätze doppelter Anführungszeichen einschließen. Angenommen, Sie möchten die View-Komponente in einem Pfad installieren, dessen Name Leerzeichen enthält. Beispiel: `VMware-viewconnectionserver-4.5.`*`x-xxxxxx`*`.exe /s /v"`*`Befehlszeilenoptionen`* `INSTALLDIR=""d:\abc\my folder"""` In diesem Beispiel übergibt das MSI-Installationsprogramm den Verzeichnispfad für die Installation und versucht nicht, die Zeichenfolge als Befehlszeilenoptionen auszuwerten. Beachten Sie die zweifach gesetzten doppelten Anführungszeichen, die die gesamte Befehlszeile umschließen. Die Option `/v"`*`Befehlszeilenoptionen`*`"` ist erforderlich, um eine unbeaufsichtigte Installation auszuführen.

Sie steuern den verbleibenden Teil einer unbeaufsichtigten Installation, indem Sie Befehlszeilenoptionen und MSI-Eigenschaften an das MSI-Installationsprogramm (`msiexec.exe`) übergeben. Das MSI-Installationsprogramm umfasst den Installationscode der View-Komponente. Der Installer verwendet die in die Befehlszeile eingegebenen Werte und Optionen, um die Installationsauswahl und die für die View-Komponente spezifischen Setup-Optionen auszuwerten.

Tabelle 5-6 zeigt die Befehlszeilenoptionen und MSI-Eigenschaftenwerte, die an das MSI-Installationsprogramm übergeben werden.

Tabelle 5-6. MSI-Befehlszeilenoptionen und MSI-Eigenschaften

MSI-Option oder -Eigenschaft	Beschreibung
`/qn`	Weist das MSI-Installationsprogramm an, keine Seiten des Installations-Assistenten anzuzeigen. Angenommen, Sie möchten View Agent unbeaufsichtigt installieren und nur standardmäßige Setup-Optionen und Funktionen verwenden: `VMware-viewagent-4.5.x-xxxxxx.exe /s /v"/qn"` Alternativ können Sie die Option `/qb` verwenden, um die Assistentenseiten in einer nicht interaktiven, automatisierten Installation anzuzeigen. Im Verlauf der Installation werden die Assistentenseiten angezeigt, eine Eingabe ist jedoch nicht möglich. Die Option `/qn` oder `/qb` ist erforderlich, um eine unbeaufsichtigte Installation auszuführen.
`INSTALLDIR`	Gibt einen alternativen Installationspfad für die View-Komponente an. Verwenden Sie das Format *`INSTALLDIR=Pfad`*, um den Installationspfad anzugeben. Sie können diese MSI-Eigenschaft ignorieren, wenn Sie die View-Komponente im Standardpfad installieren möchten. Diese MSI-Eigenschaft ist optional.
`ADDLOCAL`	Legt die komponentenspezifischen Funktionen fest, die installiert werden sollen. In einer interaktiven Installation zeigt das View-Installationsprogramm Auswahloptionen für das benutzerdefinierte Setup an. Mithilfe der MSI-Eigenschaft `ADDLOCAL` können Sie diese Setup-Optionen an der Befehlszeile angeben. Um alle verfügbaren Optionen für ein benutzerdefiniertes Setup zu installieren, geben Sie `ADDLOCAL=ALL` ein. Beispiel: `VMware-viewagent-4.5.x-xxxxxx.exe /s /v"/qn ADDLOCAL=ALL"` Wenn Sie die MSI-Eigenschaft `ADDLOCAL` nicht verwenden, werden die standardmäßigen Setup-Optionen installiert. Zur Festlegung einzelner Setup-Optionen geben Sie eine Liste der Setup-Optionen ein. Trennen Sie hierbei die Namen der Optionen durch Kommata. Verwenden Sie zwischen den Namen keine Leerzeichen. Verwenden Sie das Format *`ADDLOCAL=Wert,Wert,Wert....`* Angenommen, Sie möchten View Agent mit den View Composer-Agent- und PCoIP-Funktionen in einem Gastbetriebssystem installieren: `VMware-viewagent-4.5.x-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,SVIAgent,PCoIP"` **Hinweis** Die Funktion `Core` ist in View Agent erforderlich. Diese MSI-Eigenschaft ist optional.
`/l*v` *`Protokolldatei`*	Schreibt Protokollinformationen in die angegebene Protokolldatei. Hierbei ist eine ausführliche Ausgabe festgelegt. Beispiel: `/l*v ""%TEMP%\vmmsi.log""` In diesem Beispiel wird eine ausführliche Protokolldatei ähnlich dem Protokoll generiert, das bei einer interaktiven Installation erstellt wird. Sie können mit dieser Option benutzerdefinierte Funktionen erfassen, die möglicherweise nur für Ihre Installation gelten. Sie können die protokollierten Informationen verwenden, um Installationsfunktionen in zukünftigen unbeaufsichtigten Installationen anzugeben. Die Option `/l*v` ist optional.

Unbeaufsichtigtes Deinstallieren von View-Produkten mithilfe von MSI-Befehlszeilenoptionen

Sie können View-Komponenten mithilfe von Microsoft Windows Installer (MSI)-Befehlszeilenoptionen deinstallieren.

Syntax

`msiexec.exe /qb /x` *`produkt_code`*

Optionen

Die Option `/qb` zeigt den Deinstallationsfortschrittsbalken an. Um die Anzeige des Deinstallationsfortschrittsbalkens zu unterdrücken, ersetzen Sie die Option `/qb` durch die Option `/qn`.

Mit der Option `/x` wird die View-Komponente deinstalliert.

Die Zeichenfolge *produkt_code* kennzeichnet die View-Komponentenproduktdateien für das MSI-Deinstallationsprogramm. Sie finden die Zeichenfolge *produkt_code*, wenn Sie in der während der Installation erstellten Datei `%TEMP%\vmmsi.log` nach `ProductCode` suchen.

Informationen zu MSI-Befehlszeilenoptionen finden Sie unter „Microsoft Windows Installer-Befehlszeilenoptionen“, auf Seite 54.

Beispiele

Deinstallieren einer View Connection Server-Instanz.

```
msiexec.exe /qb /x {D6184123-57B7-26E2-809B-090435A8C16A}
```

Konfigurieren von Benutzerkonten für vCenter Server und View Composer

Um vCenter Server mit View Manager einzusetzen, müssen Sie ein Benutzerkonto mit Berechtigungen zum Ausführen von Vorgängen in vCenter Server erstellen. Wenn Sie View Composer verwenden, müssen Sie diesem vCenter Server-Benutzer zusätzliche Berechtigungen gewähren. Zur Verwaltung von Desktops, die in einem lokalen Modus verwendet werden, müssen Sie diesem Benutzer zusätzliche Berechtigungen zu den erforderlichen Berechtigungen für View Manager und View Composer erteilen.

Darüber hinaus müssen Sie in Active Directory einen Domänenbenutzer für View Composer erstellen. Siehe „Erstellen eines Benutzerkontos für View Composer“, auf Seite 25.

Einsatz der vCenter Server-Benutzer und -Domänenbenutzer für View Composer

Nachdem Sie diese zwei Benutzerkonten erstellt und konfiguriert haben, geben Sie die Benutzernamen in View Administrator an.

- Sie geben einen vCenter Server-Benutzer an, wenn Sie vCenter Server zu View Manager hinzufügen.
- Sie geben einen Domänenbenutzer für View Composer an, wenn Sie View Composer für vCenter Server konfigurieren.
- Sie geben den Domänenbenutzer für View Composer an, wenn Sie Linked-Clone-Pools erstellen.

Konfigurieren eines vCenter Server-Benutzers für View Manager, View Composer und lokalen Modus

Um ein Benutzerkonto zu konfigurieren, das die Verwendung von View Manager in vCenter Server ermöglicht, müssen Sie diesem Benutzer eine Rolle mit geeigneten Berechtigungen zuweisen. Zur Benutzung des View Composer-Dienstes in vCenter Server müssen Sie dem Benutzerkonto zusätzliche Berechtigungen erteilen. Zum Verwalten von Desktops, die im lokalen Modus verwendet werden, müssen Sie dem Benutzerkonto Berechtigungen erteilen, die Berechtigungen für View Manager, View Composer und lokalen Modus beinhalten.

Zur Unterstützung von View Composer müssen Sie diesen Benutzer auch als lokalen Systemadministrator auf dem vCenter Server-Computer konfigurieren.

Voraussetzungen

- Erstellen Sie in Active Directory einen Benutzer in der View Connection Server-Domäne oder einer vertrauenswürdigen Domäne. Siehe „Erstellen eines Benutzerkontos für vCenter Server“, auf Seite 25.
- Machen Sie sich mit den Berechtigungen vertraut, die für das Benutzerkonto erforderlich sind. Siehe „Erforderliche View Manager-Berechtigungen für den vCenter Server-Benutzer“, auf Seite 58.
- Wenn Sie View Composer verwenden, machen Sie sich mit den zusätzlich erforderlichen Berechtigungen vertraut. Siehe „Erforderliche View Composer-Berechtigungen für den vCenter Server-Benutzer“, auf Seite 59.
- Wenn Sie lokale Desktops verwalten, machen Sie sich mit den zusätzlich erforderlichen Berechtigungen vertraut. Siehe „Erforderliche Berechtigungen für den lokalen Modus für den vCenter Server-Benutzer“, auf Seite 59.

Vorgehensweise

1 Bereiten Sie in vCenter Server eine Rolle mit den erforderlichen Berechtigungen für den Benutzer vor.

   - Sie können die vordefinierte Administratorrolle in vCenter Server verwenden. Diese Rolle kann alle Aufgaben in vCenter Server ausführen.
   - Wenn Sie View Composer verwenden, können Sie eine eingeschränkte Rolle mit den Mindestberechtigungen erstellen, die View Manager und View Composer zur Durchführung von vCenter Server-Vorgängen benötigen.

     Klicken Sie in vSphere Client auf **[Administration (Verwaltung)] > [Roles (Rollen)] > [Add Role (Rolle hinzufügen)]**, geben Sie einen Rollennamen wie beispielsweise **`View Composer-Administrator`** ein und wählen Sie Berechtigungen für die Rolle aus.

     Diese Rolle muss über alle Berechtigungen verfügen, die sowohl View Manager als auch View Composer benötigen, um in vCenter Server zu agieren.
   - Wenn Sie lokale Desktops verwalten, können Sie eine eingeschränkte Rolle mit den Mindestberechtigungen erstellen, die View Manager, View Composer und die Funktion für den lokalen Modus zur Durchführung von vCenter Server-Vorgängen benötigen.

     Klicken Sie in vSphere Client auf **[Administration (Verwaltung)] > [Roles (Rollen)] > [Add Role (Rolle hinzufügen)]**, geben Sie einen Rollennamen wie beispielsweise **`Administrator für den lokalen Modus`** ein und wählen Sie Berechtigungen für die Rolle aus.

     Diese Rolle muss über alle Berechtigungen verfügen, die View Manager, View Composer und die Funktion für den lokalen Modus benötigen, um in vCenter Server zu agieren.
   - Wenn Sie View Manager ohne View Composer verwenden und keine lokalen Desktops verwalten, können Sie eine noch eingeschränktere Rolle mit den Mindestberechtigungen erstellen, die View Manager zur Ausführung von vCenter Server-Vorgängen benötigt.

     Klicken Sie in vSphere Client auf **[Administration (Verwaltung)] > [Roles (Rollen)] > [Add Role (Rolle hinzufügen)]**, geben Sie einen Rollennamen wie beispielsweise **`View Manager-Administrator`** ein und wählen Sie Berechtigungen für die Rolle aus.

2 Klicken Sie in vSphere Client mit der rechten Maustaste auf das Rechenzentrum bzw. den Cluster, das/der die virtuellen Maschinen mit den View-Desktops in Ihrer Bereitstellung hostet, klicken Sie auf **[Add Permission (Berechtigung hinzufügen)]** und fügen Sie den vCenter Server-Benutzer hinzu.

3 Wählen Sie im Dropdown-Menü die Administratorrolle oder die View Composer- bzw. View Manager-Rolle aus, die Sie erstellt haben, und weisen Sie sie dem vCenter Server-Benutzer zu.

4 Wenn Sie View Composer auf dem vCenter Server-Computer verwenden, fügen Sie das vCenter Server-Benutzerkonto der Gruppe der lokalen Systemadministratoren hinzu.

   View Composer erfordert, dass der vCenter Server-Benutzer ein Systemadministrator auf dem vCenter Server-Computer ist.

Weiter

Geben Sie beim Hinzufügen von vCenter Server zu View Manager in View Administrator den vCenter Server-Benutzer an. Siehe „Hinzufügen von vCenter Server-Instanzen zu View Manager“, auf Seite 62.

Erforderliche View Manager-Berechtigungen für den vCenter Server-Benutzer

Der vCenter Server-Benutzer muss über ausreichende Berechtigungen zur Aktivierung von View Manager für den Betrieb in vCenter Server verfügen. Erstellen Sie für den vCenter Server-Benutzer eine View Manager-Rolle mit den erforderlichen Berechtigungen.

Tabelle 5-7. View Manager-Berechtigungen

Berechtigungsgruppe	Zu aktivierende Berechtigungen
[Folder (Ordner)]	**[Create Folder (Ordner erstellen)]** **[Delete Folder (Ordner löschen)]**
[Virtual Machine (Virtuelle Maschine)]	In **[Configuration (Konfiguration)]** : ■ **[Add or remove device (Gerät hinzufügen oder entfernen)]** ■ **[Advanced (Erweitert)]** ■ **[Modify Device Settings (Geräteeinstellungen ändern)]** In **[Interaction (Interaktion)]** : ■ **[Power Off (Ausschalten)]** ■ **[Power On (Einschalten)]** ■ **[Reset (Zurücksetzen)]** ■ **[Suspend (Anhalten)]** In **[Inventory (Bestandsliste)]** : ■ **[Create new (Neue erstellen)]** ■ **[Remove (Entfernen)]** In **[Provisioning (Bereitstellung)]** : ■ **[Customize (Anpassen)]** ■ **[Deploy template (Vorlage bereitstellen)]** ■ **[Read customization specifications (Anpassungsspezifikation lesen)]**
[Resource (Ressource)]	**[Assign virtual machine to resource pool (Virtuelle Maschine zu Ressourcenpool zuweisen)]**

Erforderliche View Composer-Berechtigungen für den vCenter Server-Benutzer

Zur Unterstützung von View Composer muss der vCenter Server-Benutzer neben den zur Unterstützung von View Manager erforderlichen Berechtigungen über zusätzliche Berechtigungen verfügen. Erstellen Sie für den vCenter Server-Benutzer eine View Composer-Rolle mit den View Manager-Berechtigungen und diesen zusätzlichen Berechtigungen.

Tabelle 5-8. View Composer-Berechtigungen

Berechtigungsgruppe	Zu aktivierende Berechtigungen
[Datastore (Datenspeicher)]	**[Allocate space (Speicherplatz zuordnen)]** **[Browse datastore (Datenspeicher durchsuchen)]** **[Dateioperationen auf unterer Systemebene]**
[Virtual machine (Virtuelle Maschine)]	**[Inventory (Bestandsliste)]** (alle) **[Configuration (Konfiguration)]** (alle) **[State (Status)]** (alle) In **[Provisioning (Bereitstellung)]** : ■ **[Clone virtual machine (Virtuelle Maschine klonen)]** ■ **[Allow disk access (Festplattenzugriff zulassen)]**
[Resource (Ressource)]	**[Assign virtual machine to resource pool (Virtuelle Maschine zu Ressourcenpool zuweisen)]**
[Global]	**[Enable methods (Methoden aktivieren)]** **[Disable methods (Methoden deaktivieren)]** **[System tag (Systemkennzeichen)]**
[Network (Netzwerk)]	(alle)

Erforderliche Berechtigungen für den lokalen Modus für den vCenter Server-Benutzer

Zur Verwaltung von Desktops, die im lokalen Modus verwendet werden, benötigt der vCenter Server-Benutzer zusätzliche Berechtigungen zu den erforderlichen Berechtigungen für View Manager und View Composer. Erstellen Sie eine Administrator-Rolle für den lokalen Modus für den vCenter Server-Benutzer, in der die Berechtigungen für View Manager, View Composer und lokalen Modus kombiniert werden.

Tabelle 5-9. Berechtigungen für den lokalen Modus

Berechtigungsgruppe	Zu aktivierende Berechtigungen
[Global]	**[Set custom attribute (Benutzerdefiniertes Attribut festlegen)]**
[Host]	In **[Configuration (Konfiguration)]** : **[System management (Systemverwaltung)]**

Anfängliches Konfigurieren von View Connection Server

Nach der Installation von View Connection Server müssen Sie eine Produktlizenz installieren, vCenter Server und View Composer-Dienste zu View Manager hinzufügen, bei Bedarf Sicherheitsserver hinzufügen und externe URLs für Client-Desktops festlegen, die außerhalb Ihres Netzwerks ausgeführt werden.

View Administrator und View Connection Server

View Administrator stellt eine Verwaltungsschnittstelle für View Manager bereit.

Abhängig von Ihrer View-Bereitstellung können Sie eine oder mehrere View Administrator-Schnittstellen verwenden.

- Verwenden Sie eine View Administrator-Schnittstelle zum Verwalten der View-Komponenten, die mit einer einzelnen, eigenständigen View Connection Server-Instanz oder einer Gruppe replizierter View Connection Server-Instanzen verknüpft sind.

  Sie können die IP-Adresse einer beliebigen replizierten Instanz verwenden, um sich an View Administrator anzumelden.

- Sie müssen eine separate View Administrator-Schnittstelle zum Verwalten der View-Komponenten für jede einzelne, eigenständige View Connection Server-Instanz und jede Gruppe replizierter View Connection Server-Instanzen verwenden.

Sie verwenden View Administrator außerdem zum Verwalten von Sicherheitsservern und View Transfer Server-Instanzen, die mit View Connection Server verknüpft sind.

- Jeder Sicherheitsserver ist mit einer View Connection Server-Instanz verknüpft.
- Jede View Transfer Server-Instanz kann mit einer beliebigen View Connection Server-Instanz in einer Gruppe replizierter Instanzen kommunizieren.

Anmelden an View Administrator

Zum Ausführen anfänglicher Konfigurationsaufgaben müssen Sie sich an View Administrator anmelden.

Voraussetzungen

- Stellen Sie sicher, dass View Connection Server auf einem dedizierten Computer installiert ist.
- Vergewissern Sie sich, dass Sie einen von View Administrator unterstützten Webbrowser verwenden. Siehe „View Administrator-Anforderungen“, auf Seite 9.

Vorgehensweise

1 Öffnen Sie Ihren Webbrowser und geben Sie die folgende URL ein. Hierbei steht *Server* für den Hostnamen oder die IP-Adresse der View Connection Server-Instanz:

```
https://Server/admin
```

Sie können unter Verwendung einer sicheren Verbindung (SSL) auf View Administrator zugreifen. Bei der ersten Verbindungsherstellung zeigt Ihr Webbrowser möglicherweise eine Warnung an, nach der das mit der Adresse verknüpfte Sicherheitszertifikat nicht durch eine vertrauenswürdige Zertifizierungsstelle ausgegeben wurde. Dieses Verhalten ist normal, da es sich bei dem zum Lieferumfang von View Connection Server gehörenden Standardzertifikat um ein selbst signiertes Zertifikat handelt.

2 Klicken Sie auf **[Ignore (Ignorieren)]** , um unter Verwendung des aktuellen SSL-Zertifikats fortzufahren.

3 Melden Sie sich mit Administratoranmeldeinformationen am View Connection Server-Computer an.

Anfänglich sind alle Benutzer, die Mitglieder der lokalen Administratorengruppe (BUILTIN\Administrators) auf dem View Connection Server-Computer sind, zur Anmeldung an View Administrator berechtigt.

Nach der Anmeldung an View Administrator können Sie über **[View Configuration (View-Konfiguration)] > [Administrators (Administratoren)]** die Liste der View Manager-Administratoren ändern.

Installieren des View Connection Server-Lizenzschlüssels

Bevor Sie View Connection Server verwenden können, müssen Sie den Produktlizenzschlüssel eingeben.

Bei der ersten Anmeldung zeigt View Administrator die Seite **[Product Licensing and Usage (Produktlizenzierung und -verwendung)]** an.

Nachdem Sie den Lizenzschlüssel installiert haben, wird bei der Anmeldung die Dashboard-Seite angezeigt.

Sie müssen keinen Lizenzschlüssel konfigurieren, wenn Sie eine replizierte View Connection Server-Instanz oder einen Sicherheitsserver installieren. Replizierte Instanzen und Sicherheitsserver verwenden den allgemeinen Lizenzschlüssel, der in der View LDAP-Konfiguration gespeichert ist.

HINWEIS Für View Connection Server 4.*x* ist ein View 4.*x*-Lizenzschlüssel erforderlich. Ein mit View 3.*x* oder früheren Versionen bereitgestellter Lizenzschlüssel kann für das neue, mit View 4.*x* eingeführte Lizenzmodell nicht verwendet werden.

Vorgehensweise

1 Wenn das Fenster für die View-Konfiguration nicht angezeigt wird, klicken Sie im linken Navigationsbereich auf **[View Configuration (Konfiguration anzeigen)]** .

2 Klicken Sie auf **[Product Licensing and Usage (Produktlizenzierung und -verwendung)]** .

3 Klicken Sie in der Tabelle **[Product Licensing (Produktlizenzierung)]** auf **[Edit License (Lizenz bearbeiten)]** und geben Sie die Seriennummer für die View Manager-Lizenz ein.

4 Klicken Sie auf **[OK]** .

5 Überprüfen Sie das Ablaufdatum der Lizenz.

Hinzufügen von vCenter Server-Instanzen zu View Manager

Sie müssen View Manager zur Verbindungsherstellung mit den vCenter Server-Instanzen in Ihrer View-Bereitstellung konfigurieren. vCenter Server erstellt und verwaltet die virtuellen Maschinen, die View Manager als Desktop-Quellen verwendet.

Voraussetzungen

- Installieren Sie den View Connection Server-Produktlizenzschlüssel.
- Erstellen Sie einen vCenter Server-Benutzer mit Berechtigungen zum Ausführen der Vorgänge in vCenter Server, die zur Unterstützung von View Manager erforderlich sind. Wenn Sie View Composer verwenden, müssen Sie dem Benutzer zusätzliche Berechtigungen gewähren. Zur Verwaltung von Desktops, die im lokalen Modus verwendet werden, müssen Sie dem Benutzer zusätzliche Berechtigungen zu den erforderlichen Berechtigungen für View Manager und View Composer erteilen. Siehe „Konfigurieren eines vCenter Server-Benutzers für View Manager, View Composer und lokalen Modus“, auf Seite 56.

Vorgehensweise

1. Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)] > [Servers (Server)]** .
2. Klicken Sie im Fensterbereich **[vCenter Servers (vCenter Server)]** auf **[Add (Hinzufügen)]** .
3. Geben Sie im Textfeld für die Serveradresse den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse der vCenter Server-Instanz ein.

   Der FQDN umfasst den Hostnamen und den Domänennamen. Beispielsweise steht im FQDN `myserverhost.companydomain.com`, der Wert `myserverhost` für den Hostnamen und `companydomain.com` für die Domäne.

   HINWEIS Wenn Sie einen Server unter Verwendung eines DNS-Namens oder einer URL angeben, führt View Manager kein DNS-Lookup durch um zu überprüfen, ob der Server zuvor unter Verwendung seiner IP-Adresse eingegeben wurde. Es entsteht ein Konflikt, wenn eine vCenter Server-Instanz sowohl mit dem DNS-Namen als auch mit der IP-Adresse angegeben wird.
4. Geben Sie den Namen des vCenter Server-Benutzers ein.
5. Geben Sie das Kennwort für den vCenter Server-Benutzer ein.
6. (Optional) Geben Sie eine Beschreibung für diese vCenter Server-Instanz ein.
7. Um sich über eine sichere Verbindung (SSL) mit der vCenter Server-Instanz zu verbinden, müssen Sie die Option **[Connect using SSL (Verbindung über SSL)]** aktivieren. Die Verwendung einer SSL-Verbindung ist die Standardeinstellung.
8. Geben Sie die TCP-Portnummer ein.

   Der standardmäßige Port lautet 443.

9 (Optional) Klicken Sie auf **[Advanced (Erweitert)]** , um die maximale Anzahl gleichzeitiger Pool-Vorgänge in vCenter Server zu konfigurieren.

a Legen Sie die maximale Anzahl gleichzeitiger Bereitstellungsvorgänge fest.

Diese Einstellung legt die maximale Anzahl vollständiger virtueller Maschinen fest, die View Manager gleichzeitig in dieser vCenter Server-Instanz erstellen kann. Der Standardwert lautet acht. Diese Einstellung steuert nicht die Linked-Clone-Bereitstellung.

b Legen Sie die maximale Anzahl gleichzeitiger Betriebsvorgänge fest.

Diese Einstellung legt die maximale Anzahl an Betriebsvorgängen (Start, Herunterfahren, Anhalten usw.) fest, die gleichzeitig auf vollständigen virtuellen Maschinen ausgeführt werden können, die in dieser vCenter Server-Instanz von View Manager verwaltet werden. Der Standardwert lautet fünf. Diese Einstellung steuert die Betriebsvorgänge vollständiger virtueller Maschinen und verknüpfter Klone.

10 Wählen Sie, ob View Composer konfiguriert werden soll.

Option	Aktion
Sie verwenden View Composer nicht	Klicken Sie auf **[OK]** .
Sie verwenden View Composer	Konfigurieren Sie die View Composer-Einstellungen.

Weiter

Wenn diese View Connection Server-Instanz oder Gruppe replizierter View Connection Server-Instanzen mehrere vCenter Server-Instanzen verwendet, wiederholen Sie diesen Vorgang, um die weiteren vCenter Server-Instanzen hinzuzufügen.

Konfigurieren von View Composer-Einstellungen für vCenter Server

Zur Verwendung von View Composer müssen Sie View Manager mit anfänglichen Einstellungen konfigurieren, die den Einstellungen für den View Composer-Dienst entsprechen, der in vCenter Server installiert ist. View Composer ist eine Funktion von View Manager, der zugehörige Dienst wird jedoch direkt auf virtuellen Maschinen in vCenter Server ausgeführt.

HINWEIS Wenn Sie View Composer nicht verwenden, können Sie diese Aufgabe überspringen.

Voraussetzungen

- Ihr Active Directory-Administrator muss einen Domänenbenutzer mit Berechtigungen zum Hinzufügen und Entfernen virtueller Maschinen aus der Active Directory-Domäne erstellen, die Ihre Linked-Clone-Desktops enthält. Zum Verwalten der Linked-Clone-Computerkonten in Active Directory muss der Domänenbenutzer über die Berechtigungen **Create Computer Objects (Computerobjekte erstellen)**, **Delete Computer Objects (Computerobjekte löschen)** und **Write All Properties (Alle Eigenschaften schreiben)** verfügen.

  Siehe „Erstellen eines Benutzerkontos für View Composer“, auf Seite 25.

- Sie müssen View Manager zur Verbindungsherstellung mit vCenter Server konfigurieren. Siehe „Hinzufügen von vCenter Server-Instanzen zu View Manager“, auf Seite 62.

Vorgehensweise

1 Öffnen Sie in View Administrator das Dialogfeld **[Edit vCenter Server (vCenter Server bearbeiten)]** .

   a Klicken Sie auf **[View Configuration (View-Konfiguration)]** > **[Servers (Server)]** .

   b Wählen Sie im Fensterbereich **[vCenter Servers (vCenter Server)]** den Eintrag für vCenter Server.

   c Klicken Sie auf **[Edit (Bearbeiten)]** .

2 Wählen Sie die Option **[Enable View Composer (View Composer aktivieren)]** aus und stellen Sie sicher, dass die Portnummer mit derjenigen übereinstimmt, die Sie beim Installieren des View Composer-Dienstes in vCenter Server angegeben haben.

   View Manager überprüft, ob der View Composer-Dienst auf der vCenter Server-Instanz ausgeführt wird.

3 Klicken Sie auf **[Add (Hinzufügen)]** , um die Kontoinformationen für den Domänenbenutzer für View Composer hinzuzufügen.

   a Geben Sie den Domänennamen der Active Directory-Domäne ein.

      Beispiel: `domain.com`

   b Geben Sie den Domänenbenutzernamen ein, einschließlich des Domänennamens.

      Beispiel: `domain.com\admin`

   c Geben Sie das Kontokennwort ein.

   d Klicken Sie auf **[OK]** .

   e Um Domänenbenutzerkonten mit Berechtigungen in weiteren Active Directory-Domänen hinzuzufügen, in denen Sie Linked-Clone-Pools bereitgestellt haben, wiederholen Sie die vorangehenden Schritte.

4 Klicken Sie auf **[OK]** , um das Dialogfeld **[Edit vCenter Server (vCenter Server bearbeiten)]** zu schließen.

Weiter

Wiederholen Sie diesen Vorgang für jede vCenter Server-Instanz, in der View Composer-Dienste installiert sind.

Konfigurieren von View Client-Verbindungen

View Client-Instanzen kommunizieren mit einem View Connection Server- oder Sicherheitsserverhost über HTTPS-Verbindungen.

Die anfängliche View Client-Verbindung zur Benutzerauthentifizierung und View-Desktop-Auswahl wird eingerichtet, wenn ein Benutzer in View Client eine IP-Adresse angibt. Wenn Firewall und Lastausgleichssoftware in Ihrer Netzwerkumgebung ordnungsgemäß konfiguriert sind, wird diese Anforderung an den View Connection Server- oder Sicherheitsserverhost gesendet.

Wenn Benutzer sich über das Microsoft RDP-Anzeigeprotokoll mit einem View-Desktop verbinden, baut View Client eine zweite HTTPS-Verbindung mit dem View Connection Server- oder Sicherheitsserverhost auf. Diese Verbindung wird als „Tunnelverbindung“ bezeichnet, da sie einen sicheren Tunnel für die Übertragung von RDP-Daten bereitstellt.

Wenn die Tunnelverbindung deaktiviert ist, werden – unter Umgehung des View Connection Server- oder Sicherheitsserverhosts – View-Desktop-Sitzungen direkt zwischen dem Clientsystem und der virtuellen Maschine mit dem View-Desktop aufgebaut. Dieser Verbindungstyp wird als direkte Verbindung bezeichnet.

Clients mit den Anzeigeprotokollen PCoIP und HP RGS nutzen die Tunnelverbindung nicht.

Konfigurieren der Tunnelverbindung

Sie verwenden View Administrator zum Konfigurieren der Tunnelverbindung.

Nur Clients, die das RDP-Anzeigeprotokoll verwenden, können die Tunnelverbindung nutzen. Clients mit den Anzeigeprotokollen PCoIP und HP RGS nutzen die Tunnelverbindung nicht.

Vorgehensweise

1 Wählen Sie in View Administrator **[View Configuration (Konfiguration anzeigen)] > [Servers (Server)]** .

2 Wählen Sie unter **[View Connection Servers (View Connection Server)]** eine View Connection Server-Instanz aus und klicken Sie auf **[Edit (Bearbeiten)]** .

- Wählen Sie zum Konfigurieren eines sicheren Tunnels zur Übertragung von RDP-Daten zwischen virtuellen View-Desktop-Maschinen und dem View Connection Server- bzw. Sicherheitsserverhost die Option **[Use secure tunnel connection to desktop (Sichere Tunnelverbindung zum Desktop verwenden)]** .
- Um View Connection Server bzw. Sicherheitsserverhost zu umgehen und direkte Verbindungen zwischen Clientsystemen und virtuellen View-Desktop-Maschinen zu konfigurieren, deaktivieren Sie **[Use secure tunnel connection to desktop (Sichere Tunnelverbindung zum Desktop verwenden)]** .

3 Klicken Sie auf **[OK]** , um Ihre Änderungen zu speichern.

Konfigurieren externer URLs für Tunnelverbindungen

Zur Verwendung der Tunnelverbindung muss ein Clientsystem in der Lage sein, den vollqualifizierten Domänennamen (FQDN) des View Connection Server- oder Sicherheitsserverhosts aufzulösen. In der Standardeinstellung kann der View Connection Server- oder Sicherheitsserverhost nur über Tunnelclients kontaktiert werden, die sich innerhalb desselben Netzwerks befinden und daher in der Lage sind, den angeforderten Server zu ermitteln.

Viele Organisationen erfordern, dass Benutzer sich von einem externen Standort aus verbinden können. Hierzu wird entweder ein Domänen- oder Subdomänenname bzw. eine IP-Adresse verwendet, der/die extern auflösbar ist, oder spezifische Ports werden einer vorhandenen Adresse neu zugeordnet, um Clientanforderungen an den geeigneten Server umzuleiten (typischerweise an einen Sicherheitsserver). Beispiel:

- `https://view-example.com:443`
- `https://view.example.com:443`
- `https://example.com:1234`

Zur Verwendung solcher Adressen in View Manager müssen Sie den View Connection Server- oder Sicherheitsserverhost zur Rückgabe einer externen URL anstelle eines FQDN konfigurieren.

Das Vorgehen zum Konfigurieren einer externen URL ist für View Connection Server-Instanzen und Sicherheitsserver unterschiedlich.

- Für eine View Connection Server-Instanz legen Sie eine externe URL fest, indem Sie die View Connection Server-Einstellungen in View Administrator bearbeiten.
- Für einen Sicherheitsserver legen Sie eine externe URL fest, wenn Sie das View Connection Server-Installationsprogramm ausführen. Sie können mithilfe von View Administrator die externe URL für einen Sicherheitsserver ändern.

Festlegen der externen URL für eine View Connection Server-Instanz

Sie verwenden View Administrator, um die externe URL für eine View Connection Server-Instanz zu konfigurieren. Tunnelclients, die außerhalb Ihres Netzwerks ausgeführt werden, müssen eine extern auflösbare URL zur Verbindungsherstellung mit einer View Connection Server-Instanz verwenden.

Für Sicherheitsserver konfigurieren Sie die externe URL im View Connection Server-Installationsprogramm.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)] > [Servers (Server)]** .

2 Wählen Sie unter **[View Connection Servers (View Connection Server)]** eine View Connection Server-Instanz aus und klicken Sie auf **[Edit (Bearbeiten)]** .

3 Geben Sie im Feld **[External URL (Externe URL)]** die externe URL ein.

Die URL muss das Protokoll, den extern auflösbaren Hostnamen und die Portnummer enthalten.

Beispiel: `https://view.example.com:443`

4 Klicken Sie auf **[OK]** .

Ändern der externen URL für einen Sicherheitsserver

Verwenden Sie View Administrator, um die externe URL für einen Sicherheitsserver zu ändern.

Sie konfigurieren die externe URL für einen Sicherheitsserver anfänglich im View Connection Server-Installationsprogramm.

Voraussetzungen

Stellen Sie sicher, dass der Sicherheitsserver auf View Connection Server 4.5 aktualisiert ist.

Vorgehensweise

1 Wählen Sie in View Administrator **[View Configuration (Konfiguration anzeigen)] > [Servers (Server)]** .

2 Wählen Sie im Bereich **[Security Servers (Sicherheitsserver)]** den gewünschten Sicherheitsserver und klicken Sie auf **[Edit (Bearbeiten)]** .

Die Schaltfläche **[Edit (Bearbeiten)]** steht nicht zur Verfügung, wenn der Sicherheitsserver nicht auf View Connection Server 4.5 aktualisiert wurde.

3 Geben Sie im Feld **[External URL (Externe URL)]** die externe URL ein.

Die URL muss das Protokoll, den extern auflösbaren Hostnamen des Sicherheitsservers und die Portnummer enthalten.

Beispiel: `https://view.example.com:443`

4 Klicken Sie auf **[OK]** , um Ihre Änderungen zu speichern.

View Administrator sendet die aktualisierte externe URL an den Sicherheitsserver. Es ist kein Neustart des Sicherheitsserverdienstes erforderlich, damit die Änderungen wirksam werden.

Größeneinstellungen für Windows Server zur Unterstützung Ihrer Bereitstellung

Zur Unterstützung sehr umfangreicher Bereitstellungen von View Manager-Desktops können Sie die Windows Server-Computer konfigurieren, auf denen Sie View Connection Server installieren. Legen Sie in diesem Rahmen auf jedem Computer die Anzahl der kurzlebigen Ports, die TCB-Hash-Tabellengrößen, die Java Virtual Machine-Einstellungen sowie die Größe der Windows-Auslagerungsdatei fest. Durch diese Anpassungen wird sichergestellt, dass die Computer über angemessene Ressourcen zur ordnungsgemäßen Ausführung mit der erwarteten Benutzerlast verfügen.

Informationen zu den Hardware- und Arbeitsspeicheranforderungen für View Connection Server finden Sie unter „Hardwareanforderungen für View Connection Server“, auf Seite 8.

Hardware- und Arbeitsspeicherempfehlungen für den Einsatz von View Connection Server in einer umfangreichen View-Bereitstellung finden Sie unter „View Connection Server: Konfigurieren von virtuellen Maschinen und Maximalwerten“ im *Planungshandbuch für die VMware View-Architektur*.

Kurzlebige Ports

Der View Manager verwendet "kurzlebige" Ports, um TCP-Verbindungen zwischen View Connection Server und den verwalteten View-Desktops herzustellen. Zur Unterstützung einer umfangreichen View-Desktop-Bereitstellung können Sie die Anzahl der verfügbaren kurzlebigen Ports erhöhen.

Ein kurzlebiger Port ist ein vorübergehend eingesetzter Port, der durch das Betriebssystem erstellt wird, wenn ein Programm einen beliebigen verfügbaren Benutzerport anfordert. Das Betriebssystem bezieht die Portnummer aus einem vordefinierten Bereich (typischerweise zwischen 1024 und 65535) und gibt sie wieder frei, nachdem die zugehörigen TCP-Verbindungen getrennt wurden.

Standardmäßig kann das System eine Höchstzahl von etwa 4.000 kurzlebigen Ports erstellen, die gleichzeitig auf Windows Server 2003 verwendet werden, sowie etwa 16.000 Ports auf Windows Server 2008.

Auf Windows Server 2003 32-Bit-Computern sollten Sie die Anzahl der verfügbaren kurzlebigen Ports steigern, wenn eine View Connection Server-Instanz voraussichtlich mehr als 800 gleichzeitige Clientverbindungen verwendet.

Berechnen der Anzahl kurzlebiger Ports

Sie können die Anzahl kurzlebiger Ports berechnen, die auf jeder View Connection Server-Instanz benötigt werden, um eine große Anzahl an gleichzeitigen Clientverbindungen zu unterstützen.

Vorgehensweise

- Verwenden Sie die folgende Formel:

  ```
  Anzahl der kurzlebigen Ports = ((5 x Clients) / Server) + 10
  ```

  Hierbei gilt:

Clients	Voraussichtliche Anzahl der gleichzeitigen Clientverbindungen
Server	Anzahl der View Connection Server-Instanzen in der replizierten Gruppe

Beispiel 5-1. Berechnen der Anzahl kurzlebiger Ports

Angenommen, Sie planen eine Bereitstellung, die durch drei View Connection Server-Instanzen verwaltet wird. Wenn Sie in dieser Bereitstellung 3.000 Clientverbindungen unterstützen möchten, benötigen Sie 5.010 kurzlebige Ports, wie in Tabelle 5-10 dargestellt.

Tabelle 5-10. Beispiel der Berechnung der Anzahl kurzlebiger Ports

Konfigurationsparameter	Beispielwerte
Voraussichtliche Anzahl der gleichzeitigen Clientverbindungen	3,000
Anzahl der View Connection Server-Instanzen in der replizierten Gruppe	3
((5 x Clients) / Server) + 10 = Anzahl der kurzlebigen Ports auf jeder View Connection Server-Instanz	(5 x 3.000) / 3 + 10 = 5.010

Weiter

Verwenden Sie die „Arbeitsblätter zum Berechnen von kurzlebigen Ports und TCB-Hash-Tabellengröße“, auf Seite 71 zur Bereitstellung der Werte für Ihre Umgebung.

Erhöhen der Anzahl kurzlebiger Ports

Sie können die Windows-Registrierung bearbeiten, um die maximale Anzahl an kurzlebigen Ports auf einem Windows Server-Computer zu erhöhen, auf View Connection Server ausgeführt wird.

Registrierungseinträge können von Active Directory-Gruppenrichtlinien außer Kraft gesetzt werden. Verwenden Sie nach Möglichkeit eine Gruppenrichtlinie, um die maximale Anzahl an kurzlebigen Ports auf View Connection Server festzulegen.

Voraussetzungen

Berechnen Sie die Anzahl kurzlebiger Ports, die auf dem Windows Server-Computer konfiguriert werden sollten. Siehe „Berechnen der Anzahl kurzlebiger Ports“, auf Seite 67.

Ändern Sie den Wert in der Windows-Registrierung nur dann, wenn die Anzahl der berechneten Ports über 4.000 (Windows Server 2003) bzw. über 16.000 (Windows Server 2008) liegt.

Vorgehensweise

1 Starten Sie auf dem Windows Server-Computer den Windows-Registrierungs-Editor.

   a Wählen Sie **[Start] > [Command Prompt (Eingabeaufforderung)]** .

   b Geben Sie an der Eingabeaufforderung den Befehl **`regedit`** ein.

2 Suchen Sie in der Registrierung nach dem richtigen Unterschlüssel und klicken Sie auf **[Parameters (Parameter)]** .

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
```

3 Klicken Sie auf **[Edit (Bearbeiten)] > [New (Neu)]** und fügen Sie einen Registrierungseintrag hinzu.

```
Value Name (Name): MaxUserPort
Value Type (Typ): DWORD
Value data (Wert): 1024 + <berechnete Anzahl an kurzlebigen Ports>
Valid Range (Gültigkeitsbereich): 5000–65534 (dezimal)
```

4 Beenden Sie den Windows-Registrierungs-Editor.

5 Starten Sie den Windows Server-Computer neu.

Vergrößern der TCB-Hash-Tabelle

Der TCB (Transmission Control Block) enthält Informationen zu jeder TCP-Verbindung, die zwischen View Connection Server-Clients und den zugehörigen Desktops eingerichtet wird. Zur Unterstützung einer umfangreichen View-Desktop-Bereitstellung können Sie die TCB-Hash-Tabelle vergrößern.

Der TCB ist eine speicherresidente Datenstruktur, die Socket-Nummern, den Standort eingehender und ausgehender Datenpuffer, die empfangenen oder nicht bestätigten Bytes sowie weitere Informationen enthält.

Zum schnellen Abruf dieser Informationen speichert Windows Server TCB-Datenstrukturen in einer Hash-Tabelle.

Standardmäßig konfiguriert Windows Server die Anzahl der Hash-Tabellenzeilen basierend auf der Anzahl der CPUs im Windows Server-Computer.

Sie verwenden zwei unterschiedliche Formeln zum Berechnen der TCB-Hash-Tabellengröße auf View Connection Server-Instanzen und Sicherheitsservern.

Berechnen der TCB-Hash-Tabellengröße für View Connection Server-Instanzen

Zur Unterstützung einer großen Anzahl an View-Desktops können Sie die Größe der TCB-Hash-Tabelle auf jeder View Connection Server-Instanz optimieren. Berechnen Sie hierzu die Größe in Zeilen.

Vorgehensweise

- Verwenden Sie die folgende Formel:

  ```
  Anzahl der Hash-Tabellenzeilen auf jeder View Connection Server-Instanz =((5 x Clients) / Server) + Desktops + 20
  ```

  Hierbei gilt:

`Clients`	Voraussichtliche Anzahl der gleichzeitigen Clientverbindungen
`Server`	Anzahl der View Connection Server-Instanzen in der replizierten Gruppe
`Desktops`	Anzahl der View-Desktop-Quellen in Ihrer Bereitstellung

Beispiel 5-2. Berechnen der TCB-Hash-Tabellengröße auf jeder View Connection Server-Instanz

Angenommen, Sie verfügen in Ihrer Bereitstellung über 3.000 gleichzeitige Clientverbindungen, drei View Connection Server-Instanzen und 6.000 View-Desktop-Quellen.

Das Ergebnis für jede View Connection Server-Instanz ist 11.200, wie in Tabelle 5-11 gezeigt.

Tabelle 5-11. Beispiel der Berechnung der TCB-Hash-Tabellengröße auf jeder View Connection Server-Instanz

Konfigurationsparameter	Beispielwerte
Voraussichtliche Anzahl der gleichzeitigen Client-Desktop-Verbindungen	3,000
Anzahl der View Connection Server-Instanzen	3
Anzahl der View-Desktop-Quellen	6,000
((5 x Clients) / Server) + Desktops + 20 = Anzahl der TCB-Hash-Tabellenzeilen auf jedem Server	(5 x 3.000) / 3 + 6.000 + 20 = 11.020

Weiter

Verwenden Sie die „Arbeitsblätter zum Berechnen von kurzlebigen Ports und TCB-Hash-Tabellengröße“, auf Seite 71 zur Bereitstellung der Werte für Ihre Umgebung.

Berechnen der TCB-Hash-Tabellengröße für Sicherheitsserver

Zur Unterstützung einer großen Anzahl an View-Desktops können Sie die Größe der TCB-Hash-Tabelle auf jedem Sicherheitsserver optimieren. Berechnen Sie hierzu die Größe in Zeilen.

Vorgehensweise

- Verwenden Sie die folgende Formel:

  ```
  Anzahl der Hash-Tabellenzeilen = ((5 x Clients) / Sicherheitsserver ) + 10
  ```

  Hierbei gilt:

`Clients`	Voraussichtliche Anzahl der gleichzeitigen Clientverbindungen
`Sicherheitsserver`	Anzahl der Sicherheitsserver

Beispiel 5-3. Berechnen der TCB-Hash-Tabellengröße auf jedem Sicherheitsserver

Angenommen, Sie verfügen über 3.000 gleichzeitige Clientverbindungen und zwei Sicherheitsserver in Ihrer Bereitstellung.

Das Ergebnis für jeden Sicherheitsserver ist 7.510, wie in Tabelle 5-12 gezeigt.

Tabelle 5-12. Beispiel der Berechnung der TCB-Hash-Tabellengröße auf jedem Sicherheitsserver

Konfigurationsparameter	Beispielwerte
Voraussichtliche Anzahl der gleichzeitigen Client-Desktop-Verbindungen	3,000
Anzahl der Sicherheitsserver	2
((5 x Clients) / Sicherheitsserver) + 10 = Anzahl der TCB-Hash-Tabellenzeilen auf jedem Sicherheitsserver	(5 x 3.000) / 2 + 10 = 7.510

Weiter

Verwenden Sie die „Arbeitsblätter zum Berechnen von kurzlebigen Ports und TCB-Hash-Tabellengröße“, auf Seite 71 zur Bereitstellung der Werte für Ihre Umgebung.

Vergrößern der TCB-Hash-Tabelle auf einem Windows Server-Computer

Bearbeiten Sie die Windows-Registrierung, um die TCB-Hash-Tabelle auf Windows Server-Computer zu vergrößern, auf dem View Connection Server ausgeführt wird.

Registrierungseinträge können von Active Directory-Gruppenrichtlinien außer Kraft gesetzt werden. Verwenden Sie nach Möglichkeit eine Gruppenrichtlinie, um die Größe der TCB-Hash-Tabellen auf View Connection Server festzulegen.

Vorgehensweise

1. Starten Sie auf dem Windows Server-Computer den Windows-Registrierungs-Editor.
   a. Wählen Sie **[Start] > [Command Prompt (Eingabeaufforderung)]** .
   b. Geben Sie an der Eingabeaufforderung den Befehl **`regedit`** ein.
2. Suchen Sie in der Registrierung nach dem Unterschlüssel und klicken Sie auf **[Parameters (Parameter)]** .

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
   ```

3 Klicken Sie auf **[Edit (Bearbeiten)] > [New (Neu)]** und fügen Sie den folgenden Registrierungseintrag hinzu.

```
Value Name (Name): MaxHashTableSize
Value Type (Typ): DWORD
Value data (Wert): <berechnete Hash-Tabellengröße>
Valid Range (Gültigkeitsbereich): 64-65536 (dezimal)
```

4 Beenden Sie den Windows-Registrierungs-Editor.

5 Starten Sie den Windows Server-Computer neu.

Arbeitsblätter zum Berechnen von kurzlebigen Ports und TCB-Hash-Tabellengröße

Verwenden Sie diese Arbeitsblätter zum Berechnen der Anzahl an kurzlebigen Ports und der Größe der TCB-Hash-Tabelle auf jeder View Connection Server-Instanz und jedem Sicherheitsserver in Ihrer Bereitstellung.

Tabelle 5-13. Konfigurationsparameter

Konfigurationsparameter	Tragen Sie die Werte für Ihren Standort ein
Voraussichtliche Anzahl der gleichzeitigen Clientverbindungen	
Anzahl der View Connection Server-Instanzen	
Anzahl der Sicherheitsserver	
Anzahl der View-Desktop-Quellen	

Tabelle 5-14. Anzahl der kurzlebigen Ports

Anzahl der kurzlebigen Ports	Tragen Sie die Werte für Ihren Standort ein
((5 x Clients) / Server) + 10 = Anzahl der kurzlebigen Ports auf jeder View Connection Server-Instanz	

Tabelle 5-15. Größe der TCB-Hash-Tabelle für View Connection Server-Instanzen

Größe der TCB-Hash-Tabelle für View Connection Server-Instanzen	Tragen Sie die Werte für Ihren Standort ein
((5 x Clients) / Server) + Desktops + 20 = Anzahl der Hash-Tabellenzeilen auf jeder View Connection Server-Instanz	

Tabelle 5-16. Größe der TCB-Hash-Tabelle für Sicherheitsserver

Größe der TCB-Hash-Tabelle für Sicherheitsserver	Tragen Sie die Werte für Ihren Standort ein
((5 x Clients) / Sicherheitsserver) + 10 = Anzahl der Hash-Tabellenzeilen auf jedem Sicherheitsserver	

Größeneinstellung der JVM

Durch das View Connection Server-Installationsprogramm wird die Größe des JVM-Heap-Arbeitsspeichers (Java Virtual Machine) auf View Connection Server-Computern so festgelegt, dass eine große Anzahl an gleichzeitigen View-Desktop-Sitzungen unterstützt werden kann. Wird View Connection Server jedoch auf einem 32-Bit-Windows Server-Computer ausgeführt, wird die View Secure Gateway Server-Komponente mit einer eingeschränkten JVM-Heap-Größe konfiguriert. Zur ordnungsgemäßen Konfiguration Ihrer Bereitstellung können Sie den JVM-Heap auf 32-Bit-Computern vergrößern.

Auf einem 64-Bit-Windows Server-Computer mit mindestens 10 GB Arbeitsspeicher konfiguriert das Installationsprogramm einen JVM-Heap von 2 GB Größe für die View Secure Gateway Server-Komponente. Diese Konfiguration unterstützt etwa 2.000 gleichzeitige Tunnelsitzungen, die maximale Anzahl, die View Connection Server unterstützen kann. Eine Vergrößerung des JVM-Heaps auf einem 64-Bit-Computer mit 10 GB Arbeitsspeicher bietet daher keine Vorteile.

Hinweis Auf einem 64-Bit-View Connection Server-Computer werden 10 GB Arbeitsspeicher für Bereitstellungen mit 50 oder mehr View-Desktops empfohlen. Nur für kleine Proof-of-Concept-Bereitstellungen kann die Größe des Arbeitsspeichers unter 10 GB liegen.

Wenn auf einem 64-Bit-Windows Server-Computer weniger als 10 GB Arbeitsspeicher verfügbar sind, konfiguriert das Installationsprogramm einen JVM-Heap von 512 MB Größe für die View Secure Gateway Server-Komponente. Weist der Computer lediglich die Mindestanforderung von 4 GB Arbeitsspeicher auf, unterstützt diese Konfiguration etwa 500 gleichzeitige Tunnelsitzungen. Diese Konfiguration reicht zur Unterstützung kleiner Proof-of-Concept-Bereitstellungen vollkommen aus.

Wenn Sie den Arbeitsspeicher auf einem 64-Bit-Computer auf 10 GB erweitern, um eine größere Bereitstellung zu unterstützen, wird der JVM-Heap nicht durch View Connection Server vergrößert. Zur Anpassung des JVM-Heaps auf die empfohlene Größe müssen Sie View Connection Server neu installieren.

Auf einem 32-Bit-Windows Server-Computer beträgt die standardmäßige Größe des JVM-Heaps für die View Secure Gateway Server-Komponente 512 MB. Dieser JVM-Heap kann ca. 750 gleichzeitige Tunnelsitzungen unterstützen. Zur Unterstützung von mehr als 750 Sitzungen muss der Computer über mindestens 3 GB Arbeitsspeicher verfügen, und der JVM-Heap sollte auf 1 GB vergrößert werden. Ein JVM-Heap mit 1 GB unterstützt 1.500 gleichzeitige Tunnelsitzungen, die maximal von View Connection Server auf einem 32-Bit-Computer unterstützte Zahl.

Vergrößern des JVM-Heaps auf 32-Bit-Windows Server-Computern

Sie können die Windows-Registrierung bearbeiten, um den JVM-Heap auf 32-Bit-Windows Server-Computern zu vergrößern, auf denen View Connection Server installiert ist.

Wichtig Auf einem 64-Bit-Windows Server-Computer sollte die Größe des JVM-Heaps nicht geändert werden. Eine Änderung dieses Werts kann zu einem instabilen Verhalten von View Connection Server führen. Auf 64-Bit-Computern legt das View Connection Server-Installationsprogramm die Größe des JVM-Heaps in Abhängigkeit vom physischen Arbeitsspeicher fest. Wenn Sie den physischen Arbeitsspeicher auf einem 64-Bit-View Connection Server-Computer ändern, führen Sie eine Neuinstallation von View Connection Server aus, um die Größe des JVM-Heaps zurückzusetzen.

Auf einem 32-Bit-Computer müssen Sie den JVM-Heap immer dann vergrößern, wenn Sie die View Connection Server-Software installieren oder aktualisieren.

Vorgehensweise

1 Starten Sie auf dem Windows Server-Computer den Windows-Registrierungs-Editor.

   a Wählen Sie **[Start] > [Command Prompt (Eingabeaufforderung)]** .

   b Geben Sie an der Eingabeaufforderung den Befehl **`regedit`** ein.

2 Suchen Sie in der Registrierung nach dem Unterschlüssel und klicken Sie auf **[JvmOptions]** .

```
HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\wsnm\tunnelService\Params
```

3 Klicken Sie auf **[Edit (Bearbeiten)] > [Modify (Ändern)]** .

   Ein Windows-Dialogfeld mit einem Eintrag wie dem folgenden wird geöffnet:

```
–Xms128m –Xmx512m –Xss96k –Xrs –XX:+UseConcMarkSweepGC
–Dsimple.http.poller=simple.http.GranularPoller
–Dsimple.http.connect.configurator=com.vmware.vdi.front.SimpleConfigurator
```

4 Ändern Sie den Wert für Parameter `–Xmx` in **`–Xmx1024m`**.

   Das Dialogfeld zeigt den folgenden Eintrag:

```
–Xms128m –Xmx1024m –Xss96k –Xrs –XX:+UseConcMarkSweepGC
–Dsimple.http.poller=simple.http.GranularPoller
–Dsimple.http.connect.configurator=com.vmware.vdi.front.SimpleConfigurator
```

5 Klicken Sie auf **[OK]** und beenden Sie den Registrierungs-Editor.

6 Starten Sie den Windows Server-Computer neu.

Konfigurieren der Einstellungen für die Systemauslagerungsdatei

Sie können den virtuellen Arbeitsspeicher auf den Windows Server-Computern optimieren, auf denen Ihre View Connection Server-Instanzen installiert sind, indem Sie die Einstellungen für die Systemauslagerungsdatei ändern.

Bei der Installation von Windows Server berechnet Windows, basierend auf dem physischen Arbeitsspeicher, eine anfängliche und eine maximale Größe der Auslagerungsdatei. Diese Standardeinstellungen werden auch nach einem Neustart des Computers beibehalten.

Wenn es sich bei dem Windows Server-Computer um eine virtuelle Maschine handelt, können Sie die Arbeitsspeichergröße über vCenter Server ändern. Wenn Windows jedoch die Standardeinstellung verwendet, wird die Größe der Systemauslagerungsdatei nicht an die neue Arbeitsspeichergröße angepasst.

Vorgehensweise

1 Navigieren Sie auf dem Windows Server-Computer mit installiertem View Connection Server zum Dialogfeld **[Virtual Memory (Virtueller Arbeitsspeicher)]** .

   Standardmäßig ist die Einstellung **[Custom size (Benutzerdefiniert)]** ausgewählt. Es wird eine anfängliche und eine maximale Größe der Auslagerungsdatei angezeigt.

2 Klicken Sie auf **[System managed size (Größe wird vom System verwaltet)]** .

Windows berechnet, basierend auf der aktuellen Arbeitsspeicherverwendung und des verfügbaren Arbeitsspeichers, die Größe der Systemauslagerungsdatei fortlaufend neu.

Installieren von View Transfer Server 6

View Transfer Server überträgt beim Ein- und Auschecken und bei der Replikation Daten zwischen lokalen Desktops und dem Rechenzentrum. Zur Installation von View Transfer Server installieren Sie die Software auf einer virtuellen Windows Server-Maschine, fügen View Transfer Server zu Ihrer View Manager-Bereitstellung hinzu und konfigurieren das Transfer Server-Repository.

Sie müssen View Transfer Server installieren und konfigurieren, wenn Sie View Client with Local Mode auf Clientcomputern bereitstellen möchten.

Zur Installation von View Transfer Server müssen Sie über eine Lizenz verfügen und lokale Desktops verwenden.

1 Installieren von View Transfer Server auf Seite 76

View Transfer Server lädt System-Image-Dateien herunter, synchronisiert Daten zwischen lokalen Desktops und den entsprechenden Remote-Desktops im Rechenzentrum und übertragt Daten, wenn Benutzer lokale Desktops ein- und auschecken. Sie installieren View Transfer Server in einer virtuellen Maschine, auf der Windows Server ausgeführt wird.

2 Hinzufügen von View Transfer Server zu View Manager auf Seite 77

View Transfer Server kann zur Übertragung von Dateien und Daten zwischen lokalen Desktops und dem Rechenzentrum mit View Connection Server eingesetzt werden. Um diese Aufgaben mithilfe von View Transfer Server ausführen zu können, muss dieser Server zu Ihrer View Manager-Bereitstellung hinzugefügt werden.

3 Konfigurieren des Transfer Server-Repositorys auf Seite 78

Im Transfer Server-Repository werden View Composer-basierte Images für Linked-Clone-Desktops gespeichert, die im lokalen Modus ausgeführt werden. Um View Transfer Server Zugriff auf das Transfer Server-Repository zu gewähren, muss dieses in View Manager konfiguriert werden. Wenn Sie keine verknüpften View Composer-Klone im lokalen Modus verwenden, ist die Konfiguration eines Transfer Server-Repositorys nicht erforderlich.

4 Firewall-Regeln für View Transfer Server auf Seite 80

Bestimmte eingehende TCP-Ports müssen an der Firewall für View Transfer Server-Instanzen geöffnet werden.

5 Unbeaufsichtigte Installation von View Transfer Server auf Seite 80

Sie können eine unbeaufsichtigte Installation von View Transfer Server durchführen, indem Sie den Namen der Installationsdatei sowie die gewünschten Installationsoptionen an der Befehlszeile eingeben. Die unbeaufsichtigte Installation ermöglicht eine effiziente Bereitstellung von View-Komponenten in einem großen Unternehmen.

Installieren von View Transfer Server

View Transfer Server lädt System-Image-Dateien herunter, synchronisiert Daten zwischen lokalen Desktops und den entsprechenden Remote-Desktops im Rechenzentrum und übertragt Daten, wenn Benutzer lokale Desktops ein- und auschecken. Sie installieren View Transfer Server in einer virtuellen Maschine, auf der Windows Server ausgeführt wird.

Zur Laufzeit wird View Transfer Server auf einem Apache-Webserver bereitgestellt. Bei der Installation von View Transfer Server konfiguriert das Installationsprogramm den Apache-Webserver als Dienst auf der virtuellen Maschine. Der Apache-Dienst verwendet die Ports 80 und 443.

Voraussetzungen

- Stellen Sie sicher, dass Sie über lokale Administratorberechtigungen auf dem Windows Server-Computer verfügen, auf dem Sie View Transfer Server installieren möchten.
- Stellen Sie sicher, dass Ihre Installation die unter „View Transfer Server-Anforderungen“, auf Seite 12 beschriebenen Anforderungen für View Transfer Server erfüllt.
- Stellen Sie sicher, dass Sie über eine Lizenz für die Installation von View Transfer Server verfügen und lokale Desktops verwenden.
- Machen Sie sich mit den eingehenden TCP-Ports vertraut, die in der Windows-Firewall für die View Connection Server-Instanzen geöffnet werden müssen. Siehe „Firewall-Regeln für View Transfer Server“, auf Seite 80.

Vorsicht Stellen Sie sicher, dass die zum Hosten von View Transfer Server verwendete virtuelle Maschine mit einem LSI Logic Parallel-SCSI-Controller konfiguriert ist. Sie können View Transfer Server nicht auf einer virtuellen Maschine mit einem SAS- oder paravirtuellen VMware-Controller installieren.

Auf virtuellen Windows Server 2008-Maschinen ist der LSI Logic-SAS-Controller standardmäßig ausgewählt. Sie müssen diese Auswahl vor Installation des Betriebssystems in einen BusLogic- oder LSI Logic-Controller ändern.

Vorgehensweise

1. Laden Sie das Installationsprogramm für VMware View Connection Server von der VMware-Produktseite unter http://www.vmware.com/de/products/ auf den Windows Server-Computer herunter.

   Der Name der Installationsdatei lautet `VMware-viewconnectionserver-4.5.x-xxxxxx.exe` oder `VMware-viewconnectionserver-x86_64-4.5.x-xxxxxx.exe`, wobei `xxxxxx` der Build-Nummer entspricht.
2. Zum Starten des Installationsprogramms doppelklicken Sie auf die Installationsdatei.
3. Stimmen Sie den Lizenzbedingungen von VMware zu.
4. Übernehmen oder ändern Sie den Zielordner.
5. Wählen Sie **[View Transfer Server]** .
6. Konfigurieren Sie den Apache-Webserver, auf dem View Transfer Server bereitgestellt wird.

   Sie können die Standardwerte für Netzwerkdomäne, Apache-Servernamen und Administrator-E-Mail-Adresse übernehmen, die vom Installationsprogramm angeboten werden.

7 Wenn Sie View Transfer Server unter Windows Server 2008 installieren, legen Sie fest, wie der Windows-Firewall-Dienst konfiguriert werden soll.

Option	Aktion
Configure Windows Firewall automatically (Windows-Firewall automatisch konfigurieren)	Lassen Sie die Windows-Firewall durch das Installationsprogramm so konfigurieren, dass die erforderlichen eingehenden TCP-Protokollverbindungen zugelassen werden.
Do not configure Windows Firewall (Windows-Firewall nicht konfigurieren)	Konfigurieren Sie die Firewall-Regeln für Windows manuell.

Wenn Sie View Transfer Server unter Windows Server 2003 installieren, müssen Sie die erforderlichen Firewall-Regeln für Windows manuell konfigurieren.

8 Schließen Sie das Installationsprogramm ab, um View Transfer Server zu installieren.

Der VMware View Transfer Server-Dienst, der View Transfer Server-Steuerungsdienst und die VMware View-Framework-Komponentendienste werden auf der virtuellen Maschine installiert und gestartet.

Weiter

Fügen Sie View Transfer Server in View Administrator zu Ihrer View Manager-Bereitstellung hinzu.

Hinzufügen von View Transfer Server zu View Manager

View Transfer Server kann zur Übertragung von Dateien und Daten zwischen lokalen Desktops und dem Rechenzentrum mit View Connection Server eingesetzt werden. Um diese Aufgaben mithilfe von View Transfer Server ausführen zu können, muss dieser Server zu Ihrer View Manager-Bereitstellung hinzugefügt werden.

Sie können mehrere View Transfer Server-Instanzen zu View Manager hinzufügen. Die View Transfer Server-Instanzen greifen auf ein gemeinsames Transfer Server-Repository zu. Die Übertragungsarbeitslast für die lokalen Desktops, die über eine View Connection Server-Instanz oder von einer Gruppe replizierter View Connection Server-Instanzen verwaltet werden, wird auf diese View Transfer Server-Instanzen verteilt.

Hinweis Beim Hinzufügen von View Transfer Server zu View Manager wird die DRS-Automatisierungsrichtlinie (Distributed Resource Scheduler) auf **[Manual (Manuell)]** eingestellt, wodurch DRS deaktiviert wird.

Voraussetzungen

- Stellen Sie sicher, dass View Transfer Server auf einer virtuellen Windows Server-Maschine installiert ist.
- Stellen Sie sicher, dass vCenter Server zu View Manager hinzugefügt wurde. Die View Administrator-Seite **[View Configuration (View-Konfiguration)] > [Servers (Server)]** zeigt vCenter Server-Instanzen an, die zu View Manager hinzugefügt werden.

Vorgehensweise

1 Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)] > [Servers (Server)]** .

2 Klicken Sie im Fenster **[Transfer Servers (Übertragungsserver)]** auf **[Add (Hinzufügen)]** .

3 Wählen Sie im Assistenten zum Hinzufügen von Transfer Server-Instanzen die vCenter Server-Instanz, über welche die virtuelle View Transfer Server-Maschine verwaltet wird, und klicken Sie auf **[Next (Weiter)]** .

4 Wählen Sie die virtuelle Maschine, auf der View Transfer Server installiert ist, und klicken Sie auf **[Finish (Fertig stellen)]** .

   View Connection Server fährt die virtuelle Maschine herunter, konfiguriert sie mit vier SCSI-Controllern neu und führt anschließend einen Neustart für die virtuelle Maschine aus. Durch die Konfiguration mehrerer SCSI-Controller wird die Anzahl an Festplattenübertragungen erhöht, die View Transfer Server gleichzeitig ausführen kann.

Die View Transfer Server-Instanz wird im View Administrator im Fenster **[Transfer Servers (Übertragungsserver)]** angezeigt. Wenn kein Transfer Server-Repository konfiguriert ist, wird der View Transfer Server-Status von **[Pending (Ausstehend)]** in **[Missing Transfer Server Repository (Transfer Server-Repository fehlt)]** geändert. Wenn ein Transfer Server-Repository konfiguriert ist, wird der Status von **[Pending (Ausstehend)]** über **[Initializing Transfer Server repository (Transfer Server-Repository wird initialisiert)]** in **[Ready (Bereit)]** geändert.

Dieser Vorgang kann einige Minuten dauern. Sie können auf die Aktualisierungsschaltfläche im View Administrator klicken, um den aktuellen Status zu überprüfen.

Beim Hinzufügen der View Transfer Server-Instanz zu View Manager wird der Apache2.2-Dienst auf der virtuellen View Transfer Server-Maschine gestartet.

Vorsicht Wenn Ihre virtuelle View Transfer Server-Maschine eine frühere Version aufweist als Hardwareversion 7, muss nach dem Hinzufügen von View Transfer Server zu View Manager die statische IP-Adresse auf der virtuellen View Transfer Server-Maschine konfiguriert werden.

Beim Hinzufügen mehrerer SCSI-Controller zur virtuellen View Transfer Server-Maschine entfernt Windows die statische IP-Adresse und konfiguriert die virtuelle Maschine für die Verwendung von DHCP neu. Nach dem Neustart der virtuellen Maschine muss die statische IP-Adresse erneut in der virtuellen Maschine eingegeben werden.

Konfigurieren des Transfer Server-Repositorys

Im Transfer Server-Repository werden View Composer-basierte Images für Linked-Clone-Desktops gespeichert, die im lokalen Modus ausgeführt werden. Um View Transfer Server Zugriff auf das Transfer Server-Repository zu gewähren, muss dieses in View Manager konfiguriert werden. Wenn Sie keine verknüpften View Composer-Klone im lokalen Modus verwenden, ist die Konfiguration eines Transfer Server-Repositorys nicht erforderlich.

Wenn View Transfer Server in View Manager konfiguriert wird, bevor Sie das Transfer Server-Repository konfigurieren, validiert View Transfer Server während der Konfiguration den Speicherort des Transfer Server-Repositorys.

Wenn Sie mehrere View Transfer Server-Instanzen zu dieser View Manager-Bereitstellung hinzufügen möchten, konfigurieren Sie das Transfer Server-Repository auf einer Netzwerkfreigabe. Andere View Transfer Server-Instanzen können nicht auf ein Transfer Server-Repository zugreifen, das sich auf einem lokalen Laufwerk einer View Transfer Server-Instanz befindet.

Stellen Sie sicher, dass das Transfer Server-Repository groß genug ist, um Ihr View Composer-Basis-Image zu speichern. Ein Basis-Image kann eine Größe von mehreren Gigabyte aufweisen.

Wenn Sie ein Remote-Transfer Server-Repository auf einer Netzwerkfreigabe konfigurieren, müssen Sie eine Benutzer-ID mit Anmeldeinformationen für den Zugriff auf die Netzwerkfreigabe bereitstellen. Als empfohlene Vorgehensweise und zur Erhöhung der Sicherheit sollten Sie den Netzwerkzugriff auf das Transfer Server-Repository auf View-Administratoren beschränken.

Voraussetzungen

- Stellen Sie sicher, dass View Transfer Server auf einer virtuellen Windows Server-Maschine installiert ist.
- Stellen Sie sicher, dass View Transfer Server zu View Manager hinzugefügt wurde. Siehe „Hinzufügen von View Transfer Server zu View Manager“, auf Seite 77.

Hinweis Das Hinzufügen von View Transfer Server zu View Manager vor dem Konfigurieren des Transfer Server-Repositorys ist eine empfohlene Vorgehensweise, keine Anforderung.

Vorgehensweise

1 Konfigurieren Sie einen Pfad und Ordner für das Transfer Server-Repository.

Das Transfer Server-Repository kann sich auf einem lokalen Laufwerk oder auf einer Netzwerkfreigabe befinden.

Option	Aktion
Local Transfer Server repository (Lokales Transfer Server-Repository)	Erstellen Sie auf der virtuellen Maschine, auf der View Transfer Server installiert ist, einen Pfad und Ordner für das Transfer Server-Repository. Beispiel: `C:\TransferRepository\`
Remote Transfer Server repository (Remote-Transfer Server-Repository)	Konfigurieren Sie einen UNC-Pfad für die Netzwerkfreigabe. Beispiel: `\\Server.Domaene.com\TransferRepository\` Alle View Transfer Server-Instanzen, die Sie dieser View Manager-Bereitstellung hinzufügen, müssen über Netzwerkzugriff auf das freigegebene Laufwerk verfügen.

2 Klicken Sie in View Administrator auf **[View Configuration (View-Konfiguration)]** > **[Servers (Server)]** .

3 Versetzen Sie alle View Transfer Server-Instanzen in den Wartungsmodus.

a Wählen Sie im Fenster **[Transfer Servers (Übertragungsserver)]** eine View Transfer Server-Instanz aus.

b Klicken Sie auf **[Enter Maintenance Mode (In Wartungsmodus wechseln)]** und anschließend auf **[OK]** .

Der View Transfer Server-Status ändert sich in **[Maintenance mode (Wartungsmodus)]** .

c Wiederholen Sie Schritt 3a und Schritt 3b für jede Instanz.

Wenn sich alle View Transfer Server-Instanzen im Wartungsmodus befinden, werden alle aktuellen Übertragungsvorgänge gestoppt.

4 Klicken Sie im Fenster **[Transfer Servers (Übertragungsserver)]** neben dem Transfer Server-Repository auf **[None Configured (Nicht konfiguriert)]** .

5 Klicken Sie auf der Seite für das Transfer Server-Repository im Bereich **[General (Allgemein)]** auf **[Edit (Bearbeiten)]** .

6 Geben Sie den Speicherort des Transfer Server-Repositorys und weitere Informationen ein.

Option	Beschreibung
Netzwerkfreigabe	■ **[Path (Pfad)]** . Geben Sie den konfigurierten UNC-Pfad ein. ■ **[Username (Benutzername)]** . Geben Sie die Benutzer-ID eines Administrators ein, der über Anmeldeinformationen zum Zugriff auf die Netzwerkfreigabe verfügt. ■ **[Password (Kennwort)]** . Geben Sie das Administratorkennwort ein. ■ **[Domain (Domäne)]** . Geben Sie den Domänennamen der Netzwerkfreigabe im NetBIOS-Format ein. Verwenden Sie nicht das Suffix `.com`.
Lokales Dateisystem	Geben Sie den Pfad ein, den Sie auf der lokalen virtuellen Maschine für View Transfer Server konfiguriert haben.

7 Klicken Sie auf **[OK]** .

Wenn der Netzwerkpfad oder das lokale Laufwerk für das Repository falsch angegeben wurden, zeigt das Dialogfeld zum Bearbeiten des Transfer Server-Repositorys eine Fehlermeldung an, und der Speicherort kann nicht konfiguriert werden. Sie müssen einen gültigen Speicherort eingeben.

8 Wählen Sie auf der Seite **[View Configuration (View-Konfiguration)] > [Servers (Server)]** die View Transfer Server-Instanz aus und klicken Sie auf **[Exit Maintenance Mode (Wartungsmodus beenden)]** .

Der View Transfer Server-Status ändert sich in **[Ready (Bereit)]** .

Firewall-Regeln für View Transfer Server

Bestimmte eingehende TCP-Ports müssen an der Firewall für View Transfer Server-Instanzen geöffnet werden.

Wenn Sie View Transfer Server auf Windows Server 2008 installieren, kann das Installationsprogramm die erforderlichen Firewall-Regeln für Windows optional für Sie konfigurieren.

Wenn Sie View Transfer Server unter Windows Server 2003 installieren, müssen Sie die erforderlichen Firewall-Regeln für Windows manuell konfigurieren.

Tabelle 6-1 listet die eingehenden TCP-Ports auf, die an der Firewall für View Transfer Server-Instanzen geöffnet werden müssen.

Tabelle 6-1. TCP-Ports für View Transfer Server-Instanzen

Protokoll	Ports
HTTP	80
HTTPS	443

Unbeaufsichtigte Installation von View Transfer Server

Sie können eine unbeaufsichtigte Installation von View Transfer Server durchführen, indem Sie den Namen der Installationsdatei sowie die gewünschten Installationsoptionen an der Befehlszeile eingeben. Die unbeaufsichtigte Installation ermöglicht eine effiziente Bereitstellung von View-Komponenten in einem großen Unternehmen.

Festlegen von Gruppenrichtlinien zum Zulassen einer unbeaufsichtigten Installation von View Transfer Server

Bevor Sie eine unbeaufsichtigte Installation von View Transfer Server ausführen können, müssen Sie Microsoft Windows-Gruppenrichtlinien konfigurieren, um eine Installation mit erhöhten Rechten zuzulassen.

Sie müssen Windows Installer-Gruppenrichtlinien für Computer und Benutzer auf dem lokalen Computer festlegen.

Voraussetzungen

Stellen Sie sicher, dass Sie über lokale Administratorberechtigungen auf dem Windows Server-Computer verfügen, auf dem Sie View Transfer Server installieren möchten.

Vorgehensweise

1 Melden Sie sich am Windows Server-Computer an und klicken Sie auf **[Start] > [Run (Ausführen)]** .

2 Geben Sie **`gpedit.msc`** ein und klicken Sie auf **[OK]** .

3 Klicken Sie im Gruppenrichtlinienobjekt-Editor auf **[Local Computer Policy (Richtlinie für 'Lokaler Computer')] > [Computer Configuration (Computerkonfiguration)]** .

4 Erweitern Sie **[Administrative Templates (Administrative Vorlagen)]** , öffnen Sie den Ordner **[Windows Installer]** und doppelklicken Sie auf **[Always install with elevated privileges (Immer mit erhöhten Rechten installieren)]** .

5 Klicken Sie im Fenster **[Always Install with Elevated Privileges Properties (Eigenschaften von 'Immer mit erhöhten Rechten installieren')]** auf **[Enabled (Aktiviert)]** und anschließend auf **[OK]** .

6 Klicken Sie im linken Fensterbereich auf **[User Configuration (Benutzerkonfiguration)]** .

7 Erweitern Sie **[Administrative Templates (Administrative Vorlagen)]** , öffnen Sie den Ordner **[Windows Installer]** und doppelklicken Sie auf **[Always install with elevated privileges (Immer mit erhöhten Rechten installieren)]** .

8 Klicken Sie im Fenster **[Always Install with Elevated Privileges Properties (Eigenschaften von 'Immer mit erhöhten Rechten installieren')]** auf **[Enabled (Aktiviert)]** und anschließend auf **[OK]** .

Weiter

Führen Sie eine unbeaufsichtigte Installation von View Transfer Server aus.

Unbeaufsichtigte Installation von View Transfer Server

Sie können die Microsoft Windows Installer-Funktion (MSI) für die unbeaufsichtigte Installation dazu verwenden, View Transfer Server auf mehreren Windows-Computern zu installieren. Bei einer unbeaufsichtigten Installation verwenden Sie die Befehlszeile und müssen nicht auf Eingabeaufforderungen des Assistenten reagieren.

Voraussetzungen

- Stellen Sie sicher, dass Sie über lokale Administratorberechtigungen auf dem Windows Server-Computer verfügen, auf dem Sie View Transfer Server installieren möchten.
- Stellen Sie sicher, dass Ihre Installation die unter „View Transfer Server-Anforderungen“, auf Seite 12 beschriebenen Anforderungen für View Transfer Server erfüllt.
- Stellen Sie sicher, dass Sie über eine Lizenz für die Installation von View Transfer Server verfügen und lokale Desktops verwenden.
- Stellen Sie sicher, dass die virtuelle Maschine, auf der Sie View Transfer Server installieren, über Version 2.0 oder eine höhere Version des MSI-Laufzeitmoduls verfügt. Weitere Informationen finden Sie auf der Microsoft-Website.
- Machen Sie sich mit den MSI-Befehlszeilenoptionen vertraut. Siehe „Microsoft Windows Installer-Befehlszeilenoptionen“, auf Seite 54.

- Machen Sie sich mit den verfügbaren Eigenschaften für die unbeaufsichtigte Installation von View Transfer Server vertraut. Siehe „Eigenschaften für die unbeaufsichtigte Installation von View Transfer Server“, auf Seite 83.
- Stellen Sie sicher, dass die für die unbeaufsichtigte Installation erforderlichen Windows Installer-Gruppenrichtlinien auf dem Windows Server-Computer konfiguriert sind. Siehe „Festlegen von Gruppenrichtlinien zum Zulassen einer unbeaufsichtigten Installation von View Transfer Server“, auf Seite 80.

Vorsicht Stellen Sie sicher, dass die zum Hosten von View Transfer Server verwendete virtuelle Maschine mit einem LSI Logic Parallel-SCSI-Controller konfiguriert ist. Sie können View Transfer Server nicht auf einer virtuellen Maschine mit einem SAS- oder paravirtuellen VMware-Controller installieren.

Auf virtuellen Windows Server 2008-Maschinen ist standardmäßig der LSI Logic-SAS-Controller ausgewählt. Sie müssen diese Auswahl vor Installation des Betriebssystems in einen BusLogic- oder LSI Logic-Controller ändern.

Vorgehensweise

1 Laden Sie das Installationsprogramm für VMware View Connection Server von der VMware-Produktseite unter http://www.vmware.com/de/products/ auf den Windows Server-Computer herunter.

   Der Name der Installationsdatei lautet `VMware-viewconnectionserver-4.5.`*`x`*`-xxxxxx.exe` oder `VMware-viewconnectionserver-x86_64-4.5.`*`x`*`-`*`xxxxxx`*`.exe`, wobei `xxxxxx` der Build-Nummer entspricht.

2 Öffnen Sie auf dem Windows Server-Computer eine Eingabeaufforderung.

3 Geben Sie den Installationsbefehl in einer Zeile ein.

   Beispiel: `VMware-viewconnectionserver-4.5.`*`x`*`-`*`xxxxxx`*`.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=4"`

Der VMware View Transfer Server-Dienst, der View Transfer Server-Steuerungsdienst und die VMware View-Framework-Komponentendienste werden auf der virtuellen Maschine installiert und gestartet.

Weiter

Fügen Sie View Transfer Server in View Administrator zu Ihrer View Manager-Bereitstellung hinzu.

Eigenschaften für die unbeaufsichtigte Installation von View Transfer Server

Sie können spezielle Eigenschaften einschließen, wenn Sie eine unbeaufsichtigte Installation von View Transfer Server über die Befehlszeile ausführen. Sie müssen hierbei das Format *EIGENSCHAFT=Wert* einhalten, damit Microsoft Windows Installer (MSI) die Eigenschaften und Werte interpretieren kann.

Tabelle 6-2. MSI-Eigenschaften für die unbeaufsichtigte Installation von View Transfer Server

MSI-Eigenschaft	Beschreibung	Standardwert
INSTALLDIR	Der Pfad und der Ordner, in dem die View Connection Server-Software installiert wird. Beispiel: `INSTALLDIR=""D:\abc\Mein Ordner""` Die zweifach gesetzten doppelten Anführungszeichen um den Pfad sorgen dafür, dass das MSI-Installationsprogramm das Leerzeichen im Pfad ignoriert. Diese MSI-Eigenschaft ist optional.	`%ProgramFiles% \VMware, Inc. \VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	Die Art der View Connection Server-Installation: ■ **1**. Standardinstallation ■ **2**. Replikatinstallation ■ **3**. Sicherheitsserverinstallation ■ **4**. View Transfer Server-Installation Für die Installation von View Transfer Server verwenden Sie `VDM_SERVER_INSTANCE_TYPE=4` Diese MSI-Eigenschaft ist für eine Standardinstallation optional. Für alle anderen Installationsarten ist die Eigenschaft erforderlich.	1
SERVERDOMAIN	Die Netzwerkdomäne der virtuellen Maschine, auf der Sie View Transfer Server installieren. Dieser Wert entspricht der Netzwerkdomäne für den Apache-Webserver, die während einer interaktiven Installation konfiguriert wird. Beispiel: `SERVERDOMAIN=companydomain.com` Wenn Sie mit der MSI-Eigenschaft `SERVERDOMAIN` eine benutzerdefinierte Domäne für den Apache-Webserver angeben, müssen Sie auch benutzerdefinierte Werte für die Eigenschaften `SERVERNAME` und `SERVERADMIN` festlegen. Diese MSI-Eigenschaft ist optional.	–
SERVERNAME	Der Hostname der virtuellen Maschine, auf der Sie View Transfer Server installieren. Dieser Wert entspricht dem Hostnamen für den Apache-Webserver, der während einer interaktiven Installation konfiguriert wird. Beispiel: `SERVERNAME=ts1.companydomain.com` Wenn Sie mit der MSI-Eigenschaft `SERVERNAME` einen benutzerdefinierten Hostnamen für den Apache-Webserver angeben, müssen Sie auch benutzerdefinierte Werte für die Eigenschaften `SERVERDOMAIN` und `SERVERADMIN` festlegen. Diese MSI-Eigenschaft ist optional.	–

Tabelle 6-2. MSI-Eigenschaften für die unbeaufsichtigte Installation von View Transfer Server (Fortsetzung)

MSI-Eigenschaft	Beschreibung	Standardwert
SERVERADMIN	Die E-Mail-Adresse des Administrators für den Apache-Webserver, der mit View Transfer Server konfiguriert wird. Beispiel: `SERVERADMIN=admin@companydomain.com` Wenn Sie mit der MSI-Eigenschaft `SERVERADMIN` einen benutzerdefinierten Administrator für den Apache-Webserver angeben, müssen Sie auch benutzerdefinierte Werte für die Eigenschaften `SERVERDOMAIN` und `SERVERNAME` festlegen. Diese MSI-Eigenschaft ist optional.	–
FWCHOICE	Diese MSI-Eigenschaft legt fest, ob eine Firewall für die View Connection Server-Instanz konfiguriert werden soll. Mit dem Wert 1 wird eine Firewall festgelegt. Mit dem Wert 2 wird keine Firewall festgelegt. Beispiel: `FWCHOICE=1` Diese MSI-Eigenschaft ist optional.	1

Konfigurieren der Zertifikatauthentifizierung 7

Sie können die Zertifikatauthentifizierung für View Connection Server-Instanzen, Sicherheitsserver und View Transfer Server-Instanzen konfigurieren.

Dieses Kapitel behandelt die folgenden Themen:

- „Ersetzen des Standardzertifikats“, auf Seite 85
- „Hinzufügen von „keytool“ und „openssl“ zum Systempfad“, auf Seite 86
- „Exportieren eines vorhandenen Microsoft IIS-SSL-Serverzertifikats“, auf Seite 86
- „Erstellen eines neuen SSL-Zertifikats“, auf Seite 87
- „Konfigurieren einer View Connection Server-Instanz oder eines Sicherheitsservers für die Verwendung eines neuen Zertifikats“, auf Seite 91
- „Konfigurieren einer View Transfer Server-Instanz für die Verwendung eines neuen Zertifikats“, auf Seite 92
- „Konfigurieren von SSL für Clientverbindungen“, auf Seite 93
- „Konfigurieren von SSL für die View Transfer Server-Kommunikation“, auf Seite 93
- „Verwenden von Gruppenrichtlinien zur Konfiguration der Zertifikatüberprüfung in View Client“, auf Seite 94

Ersetzen des Standardzertifikats

Bei der Installation von View Connection Server wird ein SSL-Standardserverzertifikat generiert. Sie können das Standardzertifikat für Testzwecke verwenden.

Wichtig Sie sollten das Standardzertifikat so schnell wie möglich ersetzen. Das Standardzertifikat ist nicht von einer kommerziellen Zertifizierungsstelle signiert. Die Verwendung nicht zertifizierter Zertifikate kann von nicht vertrauenswürdigen Parteien dazu ausgenutzt werden, sich als Ihr Server auszugeben und Daten abzufangen.

Für View Connection Server-Instanzen, die direkte Verbindungen von Clientsystemen empfangen, ist ein SSL-Serverzertifikat erforderlich. Wenn Sie einen Sicherheitsserver als Front-End-System gegenüber den Clients verwenden, benötigt nur der mit der View Connection Server-Instanz kombinierte Sicherheitsserver ein SSL-Serverzertifikat. Ein SSL-Serverzertifikat wird ebenfalls benötigt, wenn Sie View Connection Server zur Verwendung der Smartcard-Authentifizierung konfigurieren.

View Transfer Server-Instanzen erfordern immer ein SSL-Serverzertifikat. Kommunikation und Datenübertragungen zwischen lokalen Computern und einer View Transfer Server-Instanz sind verschlüsselt, wenn Sie die SSL-Einstellungen für Vorgänge im lokalen Modus und die Desktop-Bereitstellung aktivieren.

Wenn Sie das Standardzertifikat durch ein eigenes Zertifikat ersetzt haben, verwenden Clients den in Ihrem Zertifikat enthaltenen öffentlichen Schlüssel, um die an den Server gesendeten Daten zu verschlüsseln. Wenn Ihr Zertifikat durch eine Zertifizierungsstelle signiert wurde, ist das Zertifikat für die Zertifizierungsstelle selbst in der Regel in den Browser eingebettet oder befindet sich in einer vertrauenswürdigen Datenbank, auf die der Client Zugriff hat. Nachdem ein Client das Zertifikat akzeptiert hat, sendet er als Antwort einen geheimen Schlüssel, der mit dem öffentlichen Schlüssel des Servers verschlüsselt wird. Dieser Schlüssel wird verwendet, um den Datenverkehr zwischen dem Client und dem Server zu verschlüsseln.

Sie verwenden die Dienstprogramme `keytool` und `openssl` zur Erstellung und Verwaltung von Zertifikaten für View.

Hinzufügen von „keytool“ und „openssl“ zum Systempfad

Die Dienstprogramme `keytool` und `openssl` dienen der Schlüssel- und Zertifikatverwaltung. Sie müssen die Pfade für diese Dienstprogramme zur Path-Systemumgebungsvariablen hinzufügen, sodass Sie die Dienstprogramme von einem beliebigen Verzeichnis auf Ihrem Host ausführen können.

Vorgehensweise

1 Klicken Sie auf Ihrem View Connection Server- oder Sicherheitsserverhost mit der rechten Maustaste auf **[My Computer (Arbeitsplatz)]** und wählen Sie **[Properties (Eigenschaften)]** .

   a Klicken Sie auf der Registerkarte **[Advanced (Erweitert)]** auf **[Environment Variables (Umgebungsvariablen)]** .

   b Wählen Sie in der Gruppe **[System variables (Systemvariable)]** die Option **[Path (Pfad)]** und klicken Sie auf **[Edit (Bearbeiten)]** .

   c Geben Sie den Pfad zum JRE-Verzeichnis im Textfeld **[Variable Value (Wert der Variablen)]** ein. Verwenden Sie ein Semikolon (;), um jeden Eintrag von anderen Einträgen im Textfeld zu trennen.

   Beispiel: *`Installationsverzeichnis`*`\VMware\VMware View\Server\jre\bin`

2 Klicken Sie auf Ihrem View Transfer Server-Host mit der rechten Maustaste auf **[My Computer (Arbeitsplatz)]** und wählen Sie **[Properties (Eigenschaften)]** .

   a Klicken Sie auf der Registerkarte **[Advanced (Erweitert)]** auf **[Environment Variables (Umgebungsvariablen)]** .

   b Wählen Sie in der Gruppe **[System variables (Systemvariable)]** die Option **[Path (Pfad)]** und klicken Sie auf **[Edit (Bearbeiten)]** .

   c Geben Sie den Pfad zu den JRE- und Apache-Verzeichnissen im Textfeld **[Variable Value (Wert der Variablen)]** ein. Verwenden Sie ein Semikolon (;), um jeden Eintrag von anderen Einträgen im Textfeld zu trennen.

   Beispiel: *`Installationsverzeichnis`*`\VMware\VMware View\Server\httpd\bin;`*`Installationsverzeichnis`*`\VMware\VMware View\Server\jre\bin`

3 Klicken Sie auf **[OK]** , bis das Dialogfeld mit den Windows-Systemeigenschaften geschlossen wird.

Exportieren eines vorhandenen Microsoft IIS-SSL-Serverzertifikats

Wenn Ihre Organisation bereits über ein gültiges SSL-Zertifikat verfügt, können Sie das im Lieferumfang von View Connection Server enthaltene SSL-Standardserverzertifikat durch das vorhandene Zertifikat ersetzen.

Zur Verwendung eines vorhandenen Zertifikats benötigen Sie sowohl das Zertifikat als auch den zugehörigen privaten Schlüssel. Sie müssen das Zertifikat von dem IIS-Anwendungsserver exportieren, der die zugehörige Website hostet. Windows stellt zu diesem Zweck ein Tool mit einer grafischen Benutzeroberfläche bereit.

Vorgehensweise

1 Klicken Sie auf dem IIS-Anwendungsserverhost auf **[Start] > [Programs (Programme)] > [Administrative Tools (Verwaltung)] > [Internet Information Services (IIS) Manager (Internetinformationsdienste-Manager (IIS))]** .

Der Internetinformationsdienste-Manager wird geöffnet.

2 Um die Liste der vom Server gehosteten Sites anzuzeigen, erweitern Sie den Eintrag für den lokalen Computer und klicken Sie auf **[Web Sites (Websites)]** .

3 Klicken Sie mit der rechten Maustaste auf den Eintrag für die Website, deren Zertifikat Sie exportieren möchten, und wählen Sie **[Properties (Eigenschaften)]** .

4 Klicken Sie auf der Registerkarte **[Directory Security (Verzeichnissicherheit)]** auf **[Server Certificate (Serverzertifikat)]** .

5 Sobald der Assistent für Webserverzertifikate geöffnet wird, klicken Sie auf **[Next (Weiter)]** .

6 Wählen Sie **[Export the current certificate to a .pfx file (Aktuelles Zertifikat in eine PFX-Datei exportieren)]** und klicken Sie auf **[Next (Weiter)]** .

7 Geben Sie einen Dateinamen für die Zertifikatsdatei an und klicken Sie auf **[Next (Weiter)]** .

8 Geben Sie ein Kennwort zum Verschlüsseln der zu exportierenden Informationen ein, bestätigen Sie das Kennwort und klicken Sie auf **[Next (Weiter)]** .

Das System zeigt zusammenfassende Informationen zum Zertifikat an, das Sie exportieren möchten.

9 Überprüfen Sie die angezeigten Informationen und klicken Sie auf **[Next (Weiter)] > [Finish (Fertig stellen)]** .

Weiter

Konfigurieren Sie Ihre View Connection Server-Instanz, Ihren Sicherheitsserver oder Ihre View Transfer Server-Instanz zur Verwendung des Zertifikats. Siehe „Konfigurieren einer View Connection Server-Instanz oder eines Sicherheitsservers für die Verwendung eines neuen Zertifikats“, auf Seite 91 oder „Konfigurieren einer View Transfer Server-Instanz für die Verwendung eines neuen Zertifikats“, auf Seite 92.

Erstellen eines neuen SSL-Zertifikats

Sie können ein neues Zertifikat erstellen, um das zum Lieferumfang von View Connection Server gehörende SSL-Standardserverzertifikat zu ersetzen. Wenn Sie ein neues Zertifikat erstellen, müssen Sie sich entweder für ein selbst signiertes oder durch eine Zertifizierungsstelle signiertes Zertifikat entscheiden.

Da selbst signierte Zertifikate nicht offiziell bei einer vertrauenswürdigen Zertifizierungsstelle registriert sind, kann ihre Authentizität nicht garantiert werden. Auch wenn sich selbst signierte Zertifikate für die Datenverschlüsselung zwischen Server und Client eignen, stellen Sie keine zuverlässigen Informationen zum Standort der Softwareanwendung oder zum Unternehmen bereit, das für deren Verwaltung verantwortlich ist.

Eine Zertifizierungsstelle ist eine vertrauenswürdige Drittpartei, welche die Identität des Zertifikats und seines Erstellers bestätigt. Wenn ein Zertifikat durch eine vertrauenswürdige Zertifizierungsstelle signiert wurde, werden die Benutzer nicht länger über Meldungen aufgefordert, das Zertifikat zu überprüfen, und Thin Client-Geräte können ohne zusätzliche Konfiguration eine Verbindung herstellen. Wenn Ihre Clients den Ursprung und die Integrität der empfangenen Daten überprüfen müssen, sollten Sie ein von einer Zertifizierungsstelle signiertes Zertifikat erwerben.

1 Generieren eines Schlüsselspeichers und eines Zertifikats auf Seite 88

Unabhängig davon, ob Sie ein selbst signiertes Zertifikat verwenden oder ein signiertes Zertifikat von einer Zertifizierungsstelle erwerben möchten, müssen Sie das Dienstprogramm `keytool` verwenden, um eine Schlüsselspeicherdatei und ein selbst signiertes Zertifikat zu generieren.

2 Erwerben eines signierten Zertifikats von einer Zertifizierungsstelle auf Seite 89

Zum Erwerb eines signierten Zertifikats von einer Zertifizierungsstelle müssen Sie eine CSR-Anfrage (Certificate Signing Request, CSR) erstellen. Zu Testzwecken stellen Anbieter wie Thawte, VeriSign oder GlobalSign ein kostenloses temporäres Zertifikat zur Verfügung, das auf einem nicht vertrauenswürdigen Stamm basiert.

3 Konvertieren eines PKCS#12-Zertifikats in das PKCS#7-Format auf Seite 90

Wenn Sie ein Zertifikat im PKCS#12-Format erworben haben, müssen Sie es vor dem Import in Ihre Schlüsselspeicherdatei in das PKCS#7-Format konvertieren.

4 Importieren eines signierten Zertifikats in eine Schlüsselspeicherdatei auf Seite 90

Wenn Sie ein signiertes Zertifikat von einer Zertifizierungsstelle erworben oder ein vorhandenes Microsoft IIS-SSL-Serverzertifikat exportiert haben, verwenden Sie das Dienstprogramm `keytool`, um das Zertifikat in Ihre Schlüsselspeicherdatei zu importieren.

Generieren eines Schlüsselspeichers und eines Zertifikats

Unabhängig davon, ob Sie ein selbst signiertes Zertifikat verwenden oder ein signiertes Zertifikat von einer Zertifizierungsstelle erwerben möchten, müssen Sie das Dienstprogramm `keytool` verwenden, um eine Schlüsselspeicherdatei und ein selbst signiertes Zertifikat zu generieren.

Wenn Sie erstmals eine Schlüsselspeicherdatei erstellen, ist das erste Zertifikat in der Schlüsselspeicherdatei ein selbst signiertes Zertifikat. Später, wenn Sie ein signiertes Zertifikat von einer Zertifizierungsstelle erwerben, importieren Sie die Antwortdatei von der Zertifizierungsstelle in die Schlüsselspeicherdatei und das selbst signierte Zertifikat wird ersetzt.

Voraussetzungen

Fügen Sie das Dienstprogramm `keytool` zum Systempfad auf Ihrem Host hinzu. Siehe „Hinzufügen von „keytool“ und „openssl“ zum Systempfad“, auf Seite 86.

Vorgehensweise

1 Öffnen Sie eine Eingabeaufforderung und verwenden Sie das Dienstprogramm `keytool`, um eine Schlüsselspeicherdatei zu generieren.

Beispiel: **`keytool -genkey -keyalg "RSA" -keystore keys.p12 -storetype pkcs12 -validity 360`**

2 Wenn Sie durch das Dienstprogramm `keytool` zur Eingabe Ihres Vor- und Nachnamens aufgefordert werden, geben Sie den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) des Clientcomputers ein, den Clientcomputer zur Verbindungsherstellung mit dem Host verwenden.

Option	Aktion
View Connection Server-Instanz	Geben Sie den FQDN des View Connection Server-Hosts ein, wenn Sie über eine View Connection Server-Instanz verfügen. Wenn Sie Lastausgleich verwenden, geben Sie den FQDN des Lastausgleichhosts ein.
Sicherheitsserver	Geben Sie den FQDN des Sicherheitsserverhosts ein.
View Transfer Server-Instanz	Geben Sie den FQDN des View Transfer Server-Hosts ein.

WICHTIG Wenn Sie Ihren Namen eingeben, wird das Zertifikat ungültig.

3 Nachdem das Dienstprogramm `keytool` die Schlüsselspeicherdatei erstellt hat, sichern Sie diese Datei.

Mithilfe der Sicherungsdatei können Sie bei Bedarf die Konfiguration für den Host wiederherstellen.

Weiter

Zur Verwendung des selbst signierten Zertifikats, das in der Schlüsselspeicherdatei enthalten ist, konfigurieren Sie die View Connection Server-Instanz, den Sicherheitsserver oder die View Transfer Server-Instanz für die Verwendung des Zertifikats. Siehe „Konfigurieren einer View Connection Server-Instanz oder eines Sicherheitsservers für die Verwendung eines neuen Zertifikats“, auf Seite 91 oder „Konfigurieren einer View Transfer Server-Instanz für die Verwendung eines neuen Zertifikats“, auf Seite 92.

Um das selbst signierte Zertifikat zu ersetzen, erwerben Sie ein signiertes Zertifikat von einer Zertifizierungsstelle. Siehe „Erwerben eines signierten Zertifikats von einer Zertifizierungsstelle“, auf Seite 89.

Erwerben eines signierten Zertifikats von einer Zertifizierungsstelle

Zum Erwerb eines signierten Zertifikats von einer Zertifizierungsstelle müssen Sie eine CSR-Anfrage (Certificate Signing Request, CSR) erstellen. Zu Testzwecken stellen Anbieter wie Thawte, VeriSign oder GlobalSign ein kostenloses temporäres Zertifikat zur Verfügung, das auf einem nicht vertrauenswürdigen Stamm basiert.

Bei dieser Vorgehensweise wird vorausgesetzt, dass nicht mehr als eine Verknüpfung in der Kette zwischen dem Serverzertifikat und dem Stammzertifikat vorliegt. Wenn Sie ein temporäres Zertifikat verwenden, sind möglicherweise ein oder mehrere Zwischenzertifikate vorhanden und Sie müssen eine andere Vorgehensweise wählen. Weitere Informationen finden Sie in den Anweisungen der Zertifizierungsstelle, die das temporäre Zertifikat generiert hat.

Voraussetzungen

Erstellen Sie eine Schlüsselspeicherdatei und ein selbst signiertes Zertifikat.

Vorgehensweise

1 Öffnen Sie eine Eingabeaufforderung und verwenden Sie das Dienstprogramm `keytool`, um eine CSR-Anfrage zu erstellen.

Beispiel:

```
keytool –certreq –keyalg "RSA" –file certificate.csr –keystore keys.p12 –storetype pkcs12 –storepass secret
```

Das Dienstprogramm `keytool` erstellt die CSR-Datei im aktuellen Verzeichnis.

2 Senden Sie die CSR-Datei gemäß dem geltenden Registrierungsverfahren an eine Zertifizierungsstelle und fordern Sie ein Zertifikat im PKCS#7-Format an.

Einige Zertifizierungsstellen stellen Zertifikate nur im PKCS#12-Format bereit. Wenn Sie ein Zertifikat dieses Typs herunterladen, müssen Sie es in das PKCS#7-Format konvertieren.

Nachdem Ihr Unternehmen überprüft wurde, signiert die Zertifizierungsstelle die Anfrage, verschlüsselt sie mit einem privaten Schlüssel und sendet Ihnen ein validiertes Zertifikat.

Weiter

Wenn Sie ein Zertifikat im PKCS#7-Format heruntergeladen haben, importieren Sie es in Ihre Schlüsselspeicherdatei. Siehe „Importieren eines signierten Zertifikats in eine Schlüsselspeicherdatei“, auf Seite 90.

Wenn Sie ein Zertifikat im PKCS#12-Format heruntergeladen haben, konvertieren Sie es in das PKCS#7-Format.

Konvertieren eines PKCS#12-Zertifikats in das PKCS#7-Format

Wenn Sie ein Zertifikat im PKCS#12-Format erworben haben, müssen Sie es vor dem Import in Ihre Schlüsselspeicherdatei in das PKCS#7-Format konvertieren.

Vorgehensweise

1 Klicken Sie mit der rechten Maustaste auf die Zertifikatsdatei (`.cer`) und wählen Sie **[Open With (Öffnen mit)] > [Crypto Shell Extensions (Krypto-Shellerweiterungen)]** .

2 Klicken Sie auf der Registerkarte **[Details]** auf **[Copy to File (In Datei kopieren)]** .

Der Zertifikatexport-Assistent wird geöffnet.

3 Geben Sie das PKCS#7-Format an, schließen Sie alle Zertifikate im Zertifizierungspfad ein und klicken Sie auf **[Next (Weiter)]** .

4 Geben Sie einen Dateinamen an und klicken Sie auf **[Next (Weiter)]** .

5 Klicken Sie auf **[Finish (Fertig stellen)]** , um die Datei im PKCS#7-Format zu exportieren.

HINWEIS Zertifikate, die in das PKCS#7-Format konvertiert wurden, weisen die Erweiterung `.p7b` auf.

Weiter

Importieren Sie das Zertifikat im PKCS#7-Format in Ihre Schlüsselspeicherdatei.

Importieren eines signierten Zertifikats in eine Schlüsselspeicherdatei

Wenn Sie ein signiertes Zertifikat von einer Zertifizierungsstelle erworben oder ein vorhandenes Microsoft IIS-SSL-Serverzertifikat exportiert haben, verwenden Sie das Dienstprogramm `keytool`, um das Zertifikat in Ihre Schlüsselspeicherdatei zu importieren.

Voraussetzungen

Wenn das Zertifikat im PKCS#12-Format vorliegt, konvertieren Sie es in das PKCS#7-Format.

Vorgehensweise

1 Kopieren Sie die Textdatei mit dem Zertifikat in das Verzeichnis, in dem sich Ihre Schlüsselspeicherdatei befindet, und speichern Sie die Datei unter dem Namen `certificate.p7`.

Beispiel:

```
-----BEGIN PKCS7-----
MIIF+AYJKoZIhvcNAQcCoIIF6TCCBeUCAQExADALBgk
LDCCApWgAwIBAgIQTpY7DsV1n1HeMGgMjMR2PzANBgk
i7coVx71/lCBOlFmx66NyKlZK5mObgvd2dlnsAP+nnS
EhCsdpikSpbtdo18jUubV6z1kQ71CrRQtbi/WtdqxQE
-----END PKCS7-----
```

2 Öffnen Sie eine Eingabeaufforderung und verwenden Sie das Dienstprogramm `keytool`, um das Zertifikat in Ihre Schlüsselspeicherdatei zu importieren.

Beispiel:

```
keytool -import -keystore keys.p12 -storetype pkcs12 -storepass secret -keyalg "RSA" -trust-
cacerts -file certificate.p7
```

3 Wenn Sie ein temporäres Zertifikat angegeben haben, beantworten Sie die folgende Meldung mit **`yes`**: `.... is not trusted. Install reply anyway?`.

Das Dienstprogramm `keytool` generiert diese Meldung, da temporäre Zertifikate nicht für eine Verwendung in der Produktion vorgesehen sind.

Weiter

Konfigurieren Sie Ihre View Connection Server-Instanz, Ihren Sicherheitsserver oder Ihre View Transfer Server-Instanz zur Verwendung des Zertifikats. Siehe „Konfigurieren einer View Connection Server-Instanz oder eines Sicherheitsservers für die Verwendung eines neuen Zertifikats“, auf Seite 91 oder „Konfigurieren einer View Transfer Server-Instanz für die Verwendung eines neuen Zertifikats“, auf Seite 92.

Konfigurieren einer View Connection Server-Instanz oder eines Sicherheitsservers für die Verwendung eines neuen Zertifikats

Um eine View Connection Server-Instanz oder einen Sicherheitsserver für die Verwendung eines neuen SSL-Serverzertifikats zu konfigurieren, müssen Sie Eigenschaften in der Datei `locked.properties` auf dem View Connection Server- oder dem Sicherheitsserverhost festlegen.

Voraussetzungen

Erstellen Sie ein selbst signiertes Zertifikat, exportieren Sie ein vorhandenes Microsoft IIS-SSL-Serverzertifikat oder erwerben Sie ein signiertes Zertifikat von einer Zertifizierungsstelle.

Vorgehensweise

1 Kopieren Sie die Schlüsselspeicherdatei, die Ihr Zertifikat enthält, in das SSL-Gateway-Konfigurationsverzeichnis auf dem View Connection Server- oder den Sicherheitsserverhost.

Beispiel: *Installationsverzeichnis*\VMware\VMware View\Server\sslgateway\conf\keys.p12

2 Fügen Sie die Eigenschaften `keyfile` und `keypass` zur Datei `locked.properties` im SSL-Gateway-Konfigurationsverzeichnis auf dem View Connection Server- oder Sicherheitsserverhost hinzu.

Wenn die Datei `locked.properties` noch nicht vorhanden ist, müssen Sie diese erstellen.

a Legen Sie die Eigenschaft `keyfile` auf den Namen Ihrer Schlüsselspeicherdatei fest.

Wenn Sie ein vorhandenes Microsoft IIS-SSL-Serverzertifikat exportiert haben, legen Sie die Eigenschaft `keyfile` auf den Namen Ihrer PFX-Datei fest.

b Legen Sie die Eigenschaft `keypass` auf das Kennwort für Ihre Schlüsselspeicherdatei fest.

Wenn Sie ein vorhandenes Microsoft IIS-SSL-Serverzertifikat exportiert haben, legen Sie die Eigenschaft `keypass` auf das Kennwort fest, das Sie beim Export des Zertifikats verwendet haben.

Beispiel:

```
keyfile=keys.p12
keypass=MY_PASS
```

3 Starten Sie den View Connection Server- oder Security Server-Dienst neu, damit die Änderungen wirksam werden.

Konfigurieren einer View Transfer Server-Instanz für die Verwendung eines neuen Zertifikats

Zur Konfiguration einer View Transfer Server-Instanz für die Verwendung eines neuen SSL-Serverzertifikats müssen Sie Ihre Zertifikatsdateien sowie die privaten Schlüsseldateien auf den View Transfer Server-Host kopieren.

Voraussetzungen

- Fügen Sie das Dienstprogramm `openssl` zur Systempfadvariablen auf Ihrem Host hinzu. Siehe „Hinzufügen von „keytool“ und „openssl“ zum Systempfad“, auf Seite 86.
- Erstellen Sie ein selbst signiertes Zertifikat, exportieren Sie ein vorhandenes Microsoft IIS-SSL-Serverzertifikat oder erwerben Sie ein signiertes Zertifikat von einer Zertifizierungsstelle.

Vorgehensweise

1 Öffnen Sie eine Eingabeaufforderung und verwenden Sie das Dienstprogramm `openssl`, um die private Schlüsseldatei aus Ihrer PFX- oder P12-Datei zu exportieren.

Beispiel: **`openssl pkcs12 –in filename.pfx –nocerts –out key.pem`**

2 Exportieren Sie die Zertifikatsdatei aus Ihrer PFX- oder P12-Datei.

Beispiel: **`openssl pkcs12 –in filename.pfx –clcerts –nokeys –out server.crt`**

3 Entfernen Sie das Kennwort aus dem privaten Schlüssel.

Mit diesem Schritt verhindern Sie, dass Apache bei jedem Neustart die Eingabe Ihres Kennworts anfordert.

Beispiel: **`openssl rsa –in key.pem –out server.key`**

4 Beenden Sie den View Transfer Server-Dienst.

5 Kopieren Sie die Zertifikatsdateien sowie die privaten Schlüsseldateien in das Verzeichnis *Installationsverzeichnis*\VMware\VMware View\Server\httpd\conf auf dem View Transfer Server-Host.

6 Benennen Sie die Zertifikatsdatei in `server.crt` um.

7 Benennen Sie die private Schlüsseldatei in `server.key` um.

8 Starten Sie den View Transfer Server-Dienst neu, damit die Änderungen wirksam werden.

9 Prüfen Sie, ob das Zertifikat richtig konfiguriert ist, indem Sie mithilfe Ihres Webbrowsers zur Website `https://`*`Transferserver-Hostadresse`* navigieren.

Konfigurieren von SSL für Clientverbindungen

Um festzulegen, ob für Clientverbindungen bei der Kommunikation mit View Connection Server SSL verwendet wird, konfigurieren Sie in View Administrator eine globale Einstellung. Die Einstellung wird auf View-Desktop-Clients und Clients angewendet, die View Administrator ausführen.

Globale Einstellungen werden auf alle Clientsitzungen angewendet, die von einer eigenständigen View Connection Server-Instanz oder einer Gruppe replizierter Instanzen verwaltet werden. Sie sind nicht spezifisch für eine einzelne View Connection Server-Instanz.

Wenn View Connection Server für die Smartcard-Authentifizierung konfiguriert ist, muss SSL für Clientverbindungen aktiviert sein.

SSL ist für Clientverbindungen standardmäßig aktiviert.

Hinweis Wenn Sie die Verwendung von SSL für Clientverbindungen deaktivieren, müssen Benutzer das Kontrollkästchen **[Use secure connection (SSL) (Sichere Verbindung verwenden (SSL))]** in View Client deaktivieren, bevor sie eine Verbindung mit dem View Connection Server-Host herstellen, und Administratoren müssen eine HTTP-URL zur Ausführung von View Administrator eingeben.

Vorgehensweise

1 Wählen Sie in View Administrator **[View Configuration (Konfiguration anzeigen)] > [Global Settings (Globale Einstellungen)]** und klicken Sie auf **[Edit (Bearbeiten)]** .

2 Zur Konfiguration von SSL für Clientverbindungen aktivieren oder deaktivieren Sie **[Require SSL for client connections and View Administrator (SSL für Clientverbindungen und View Administrator erforderlich)]** .

3 Klicken Sie auf **[OK]** , um Ihre Änderungen zu speichern.

4 Starten Sie den View Connection Server-Dienst neu, damit die Änderungen wirksam werden.

   In einer Gruppe replizierter View Connection Server-Instanzen können Sie den View Connection Server-Dienst auf einer beliebigen Instanz in der Gruppe neu starten.

Konfigurieren von SSL für die View Transfer Server-Kommunikation

Zur Konfiguration der Verwendung von SSL für die Kommunikation und Datenübertragung zwischen Clientcomputern, die lokale Desktops und View Transfer Server hosten, legen Sie die View Connection Server-Einstellungen in View Administrator fest.

Die SSL-Einstellungen für die View Transfer Server-Kommunikation und Datenübertragungen sind spezifisch für eine einzelne View Connection Server-Instanz. Möglicherweise möchten Sie SSL auf einer Instanz aktivieren, auf die Benutzer über das Internet zugreifen, SSL auf einer dedizierten Instanz für interne Benutzer jedoch deaktivieren.

SSL ist für die View Transfer Server-Kommunikation und Datenübertragungen standardmäßig deaktiviert.

Hinweis Die SSL-Einstellungen wirken sich nicht auf lokale Daten aus, diese werden immer verschlüsselt.

Vorgehensweise

1 Wählen Sie in View Administrator **[View Configuration (Konfiguration anzeigen)] > [Servers (Server)]** .

2 Wählen Sie die gewünschte View Connection Server-Instanz und klicken Sie auf **[Edit (Bearbeiten)]** .

3 Zur Konfiguration von SSL für die Kommunikation und Datenübertragung zwischen Clientcomputern, die lokale Desktops und View Transfer Server hosten, aktivieren oder deaktivieren Sie **[Use SSL for Local Mode operations (SSL für Vorgänge im lokalen Modus verwenden)]** .

   Diese Vorgänge umfassen das Ein- und Auschecken von Desktops und das Replizieren von Daten von Clientcomputern in das Rechenzentrum.

4 Zur Konfiguration von SSL für Übertragungen von View Composer-Basis-Image-Dateien vom Transfer Server-Repository auf Clientcomputer, die lokale Desktops hosten, aktivieren oder deaktivieren Sie **[Use SSL when provisioning desktops in Local Mode (SSL bei der Bereitstellung von Desktops im lokalen Modus verwenden)]** .

5 Klicken Sie auf **[OK]** , um Ihre Änderungen zu speichern.

Ihre Änderungen werden sofort wirksam. Sie müssen den View Transfer Server-Dienst nicht erneut starten.

Verwenden von Gruppenrichtlinien zur Konfiguration der Zertifikatüberprüfung in View Client

Sie können sicherheitsbezogene Gruppenrichtlinieneinstellungen in den ADM-Vorlagendateien zur Konfiguration von View Client (`vdm_client.adm`) dazu verwenden, um eine Überprüfung von SSL-Serverzertifikaten in View Client zu konfigurieren.

Die ADM-Vorlagendateien für View-Komponenten sind im Verzeichnis *`Installationsverzeichnis`*`\VMware \VMware View\Server\Extras\GroupPolicyFiles` auf Ihrem View Connection Server-Host installiert.

Informationen zur Verwendung der View Manager-Gruppenrichtlinieneinstellungen finden Sie im *VMware View-Administratorhandbuch*.

8 Erstellen einer Ereignisdatenbank

Sie erstellen eine Ereignisdatenbank, um Informationen zu View Manager-Ereignissen aufzuzeichnen. Wenn Sie keine Ereignisdatenbank konfigurieren, müssen Sie Informationen zu Ereignissen in der Protokolldatei nachsehen, und die Protokolldatei enthält nur sehr eingeschränkte Informationen.

Dieses Kapitel behandelt die folgenden Themen:

- „Hinzufügen einer Datenbank und eines Datenbankbenutzers für View-Ereignisse“, auf Seite 95
- „Vorbereiten einer SQL Server-Datenbank für die Ereignisberichterstellung“, auf Seite 96
- „Konfigurieren der Ereignisdatenbank“, auf Seite 97

Hinzufügen einer Datenbank und eines Datenbankbenutzers für View-Ereignisse

Sie erstellen eine Ereignisdatenbank, indem Sie sie zu einem vorhandenen Datenbankserver hinzufügen. Anschließend können Sie mithilfe von Reporting-Software für Unternehmen die Ereignisse in der Datenbank analysieren.

Der Datenbankserver für die Ereignisdatenbank kann sich auf einem View Connection Server-Host oder auf einem dedizierten Server befinden. Alternativ können Sie einen geeigneten vorhandenen Datenbankserver verwenden, beispielsweise einen Server, der eine View Composer-Datenbank hostet.

HINWEIS Sie müssen für diese Datenbank keine ODBC-Datenquelle erstellen.

Voraussetzungen

- Stellen Sie sicher, dass Sie über einen unterstützten MySQL SQL Server- oder Oracle-Datenbankserver auf einem System verfügen, auf den eine View Connection Server-Instanz zugreifen kann. Eine Liste der unterstützten Datenbankversionen finden Sie unter „Datenbankanforderungen für View Composer“, auf Seite 10.
- Stellen Sie sicher, dass Sie über die erforderlichen Datenbankberechtigungen zum Erstellen einer Datenbank und eines Benutzers auf dem Datenbankserver verfügen.
- Wenn Sie mit der Erstellung von Datenbanken auf Microsoft SQL Server-Datenbankservern nicht vertraut sind, lesen Sie die Schrittanweisungen unter „Hinzufügen einer View Composer-Datenbank zu SQL Server“, auf Seite 32.
- Wenn Sie mit der Erstellung von Datenbanken auf Oracle-Datenbankservern nicht vertraut sind, lesen Sie die Schrittanweisungen unter „Hinzufügen einer View Composer-Datenbank zu Oracle 11g oder 10g“, auf Seite 34.

Vorgehensweise

1 Fügen Sie dem Server eine neue Datenbank hinzu und geben Sie ihr einen beschreibenden Namen, z.B. "ViewEreignisse".

2 Fügen Sie einen Benutzer für diese Datenbank hinzu, der über Berechtigungen zum Erstellen von Tabellen, Ansichten und – im Falle von Oracle – Trigger und Sequenzen verfügt sowie die Berechtigung zum Ausführen von Lese- und Schreiboperationen für diese Objekte besitzt.

   Verwenden Sie für eine Microsoft SQL Server-Datenbank nicht das Sicherheitsmodell der integrierten Windows-Authentifizierung als Authentifizierungsmethode. Verwenden Sie auf jeden Fall die SQL Server-Authentifizierungsmethode.

Die Datenbank wird erstellt, das Schema jedoch nicht. Dieses wird erst erstellt, wenn Sie die Datenbank in View Administrator konfigurieren.

Weiter

Folgen Sie den Anweisungen unter „Konfigurieren der Ereignisdatenbank“, auf Seite 97.

Vorbereiten einer SQL Server-Datenbank für die Ereignisberichterstellung

Bevor Sie View Administrator zum Konfigurieren einer Ereignisdatenbank auf dem Microsoft SQL Server verwenden können, müssen Sie die richtigen TCP/IP-Eigenschaften konfigurieren und sicherstellen, dass der Server die SQL Server-Authentifizierung nutzt.

Voraussetzungen

- Erstellen einer SQL Server-Datenbank für die Ereignisberichterstellung. Siehe „Hinzufügen einer Datenbank und eines Datenbankbenutzers für View-Ereignisse“, auf Seite 95.
- Stellen Sie sicher, dass Sie über die erforderlichen Datenbankberechtigungen zum Konfigurieren der Datenbank verfügen.
- Stellen Sie sicher, dass der Datenbankserver die SQL Server-Authentifizierungsmethode nutzt. Verwenden Sie nicht die Windows-Authentifizierung.

Vorgehensweise

1 Öffnen Sie den SQL Server-Konfigurations-Manager und erweitern Sie **[SQL Server *YYYY* Network Configuration (Netzwerkkonfiguration von SQL Server *YYYY*)]** .

2 Wählen Sie **[Protocols for (Protokolle für) *Servername*]** .

3 Klicken Sie in der Liste der Protokolle mit der rechten Maustaste auf **[TCP/IP]** und wählen Sie **[Properties (Eigenschaften)]** .

4 Setzen Sie die Eigenschaft **[Enabled (Aktiviert)]** auf **[Yes (Ja)]** .

5 Stellen Sie sicher, dass ein Port zugewiesen ist, oder weisen Sie ggf. einen Port zu.

   Informationen zu statischen und dynamischen Ports sowie ihrer Zuweisung finden Sie in der Online-Hilfe zum SQL Server-Konfigurations-Manager.

6 Stellen Sie sicher, dass dieser Port nicht von einer Firewall blockiert ist.

Weiter

Verbinden Sie mittels View Administrator die Datenbank mit View Connection Server. Folgen Sie den Anweisungen unter „Konfigurieren der Ereignisdatenbank“, auf Seite 97.

Konfigurieren der Ereignisdatenbank

Die Ereignisdatenbank speichert Informationen zu View-Ereignissen nicht in einer Protokolldatei, sondern in Form von Einträgen in einer Datenbank.

Sie konfigurieren eine Ereignisdatenbank nach der Installation einer View Connection Server-Instanz. Sie müssen nur einen host in einer View Connection Server-Gruppe konfigurieren. Die verbleibenden Hosts in der Gruppe werden automatisch konfiguriert.

Sie können die Ereignisse in den Datenbanktabellen unter Verwendung von Microsoft SQL Server oder Oracle-Datenbankberichttools untersuchen. Weitere Informationen finden Sie im *VMware View Integration Guide (VMware View-Integrationshandbuch)*.

Voraussetzungen

Sie benötigen die folgenden Informationen, um eine Ereignisdatenbank zu konfigurieren:

- Den DNS-Namen oder die IP-Adresse des Datenbankservers.
- Die Art des Datenbankservers: Microsoft SQL Server oder Oracle.
- Die Portnummer, die für den Zugriff auf den Datenbankserver verwendet wird. Standardmäßig wird Port 1521 für Oracle und Port 1433 für SQL Server verwendet. Wenn es sich beim SQL Server-Datenbankserver um eine benannte Instanz handelt oder Sie SQL Server Express verwenden, müssen Sie möglicherweise die Portnummer ermitteln. Informationen zur Verbindungsherstellung mit einer benannten Instanz von SQL Server finden Sie im Microsoft KB-Artikel unter http://support.microsoft.com/kb/265808.
- Der Name der Ereignisdatenbank, die Sie auf dem Datenbankserver erstellt haben. Siehe „Hinzufügen einer Datenbank und eines Datenbankbenutzers für View-Ereignisse“, auf Seite 95.
- Den Benutzernamen und das Kennwort des Benutzers, den Sie für diese Datenbank erstellt haben. Siehe „Hinzufügen einer Datenbank und eines Datenbankbenutzers für View-Ereignisse“, auf Seite 95.

  Verwenden Sie die SQL Server-Authentifizierung für diesen Benutzer. Verwenden Sie nicht das Sicherheitsmodell der integrierten Windows-Authentifizierung als Authentifizierungsmethode.
- Ein Präfix für die Tabellen in der Ereignisdatenbank, beispielsweise VE_. Das Präfix ermöglicht eine gemeinsame Verwendung der Datenbank durch die View-Installationen.

Hinweis Die eingegebenen Zeichen müssen für die verwendete Datenbanksoftware zulässig sein. Die Syntax des Präfixes wird nicht überprüft, wenn Sie Daten in das Dialogfeld eingeben. Wenn Sie Zeichen eingeben, die für die verwendete Datenbanksoftware unzulässig sind, tritt ein Fehler auf, wenn View Connection Server versucht, eine Verbindung mit dem Datenbankserver herzustellen. Dieser Fehler und mögliche andere Fehlermeldungen, die bei einem ungültigen Datenbanknamen auftreten, werden in der Protokolldatei aufgezeichnet.

Vorgehensweise

1 Wählen Sie in View Administrator **[View Configuration (Konfiguration anzeigen)] > [Event Configuration (Ereigniskonfiguration)]** .

2 Klicken Sie im Abschnitt **[Event Database (Ereignisdatenbank)]** auf **[Edit (Bearbeiten)]** , geben Sie die erforderlichen Informationen in die dafür vorgesehenen Felder ein und klicken Sie auf **[OK]** .

3 (Optional) Klicken Sie im Fenster **[Event Settings (Ereigniseinstellungen)]** auf **[Edit (Bearbeiten)]**, ändern Sie den Wert für die Anzeigedauer von Ereignissen sowie die Anzahl der Tage zur Klassifizierung von neuen Ereignissen und klicken Sie auf **[OK]**.

Diese Einstellungen beziehen sich auf den Zeitraum, für den die Ereignisse in der View Administrator-Oberfläche angezeigt werden. Nach Ablauf dieses Zeitraums stehen die Ereignisse nur in den Verlaufsdatenbanktabellen zur Verfügung.

Das Fenster **[Database Configuration (Datenbankkonfiguration)]** zeigt die aktuelle Konfiguration der Ereignisdatenbank an.

4 Wählen Sie **[Monitoring (Überwachung)] > [Events (Ereignisse)]** um sicherzustellen, dass eine Verbindung mit der Ereignisdatenbank hergestellt werden kann.

Tritt bei der Verbindungsherstellung ein Fehler auf, wird eine Fehlermeldung angezeigt. Wenn Sie SQL Express oder eine benannte Instanz von SQL Server verwenden, müssen Sie möglicherweise die richtige Portnummer ermitteln, wie in den Voraussetzungen erwähnt.

Im Dashboard wird der Ereignisdatenbank in der Anzeige zum Systemkomponentenstatus unterhalb von **[Reporting Database (Berichtdatenbank)]** angezeigt.

Installieren und Ausführen von View Client

9

Sie können das View Client-Installationsprogramm entweder von der VMware-Website oder über View Portal abrufen, einer Seite für den Webzugriff, die von View Connection Server bereitgestellt wird. Nach der Installation von View Client können Sie verschiedene Startoptionen für die Endbenutzer festlegen.

Dieses Kapitel behandelt die folgenden Themen:

- „Installieren von View Client (Windows-basiert) oder View Client with Local Mode“, auf Seite 99
- „Starten von View Client (Windows-basiert) oder View Client with Local Mode“, auf Seite 101
- „Installieren von View Client unter Verwendung von View Portal“, auf Seite 103
- „Installieren von View Client auf Mac OS X“, auf Seite 104
- „Starten von View Client unter Mac OS X“, auf Seite 105
- „Festlegen von Voreinstellungen für die virtuelle Druckfunktion“, auf Seite 107
- „Verwenden von USB-Druckern“, auf Seite 108
- „Unbeaufsichtigte Installation von View Client“, auf Seite 108

Installieren von View Client (Windows-basiert) oder View Client with Local Mode

Endbenutzer öffnen View Client, um von einem physischen Computer eine Verbindung mit ihren virtuellen Desktops herzustellen. Sie können eine Windows-basierte Installationsdatei zum Installieren sämtlicher Komponenten von View Client ausführen.

Zusätzlich dazu, dass Endbenutzer mit View Client auf ihre virtuellen Desktops zugreifen, können Endbenutzer View Client zum Konfigurieren einiger Anzeigeoptionen verwenden, wenn der View-Administrator diese Optionen aktiviert. Beispielsweise können Endbenutzer optional ein Anzeigeprotokoll oder eine Fenstergröße wählen oder ihre aktuellen Anmeldeinformationen für die View-Authentifizierung verwenden.

View Client with Local Mode ermöglicht Endbenutzern das Herunterladen einer Kopie ihres virtuellen Desktops auf ihren lokalen Computer. Anschließend können die Endbenutzer den virtuellen Desktop sogar verwenden, wenn keine Netzwerkverbindung vorhanden ist. Die Latenz wird minimiert und die Leistung wird verbessert.

View Client with Local Mode ist die vollständig unterstützte Funktion, die in früheren Versionen eine experimentelle Funktion mit dem Namen View Client with Offline Desktop war.

Voraussetzungen

- Stellen Sie sicher, dass Sie sich als Administrator auf dem Clientsystem anmelden können.
- Stellen Sie sicher, dass das Clientsystem ein unterstütztes Betriebssystem verwendet. Siehe „Unterstützte Betriebssysteme für View Client und View Client with Local Mode“, auf Seite 16.
- Stellen Sie sicher, dass View Agent nicht installiert ist.
- Wenn Sie View Client with Local Mode installieren möchten, stellen Sie sicher, dass Ihre Lizenz View Client with Local Mode umfasst.
- Wenn Sie View Client with Local Mode installieren möchten, stellen Sie sicher, dass keins der folgenden Produkte installiert ist: VMware View Client, VMware Player, VMware Workstation, VMware ACE, VMware Server.
- Bestimmen Sie, ob der Benutzer des Clientgeräts von einem virtuellen Desktop auf lokal angeschlossene USB-Geräte zugreifen darf. Falls nicht, müssen Sie die vom Assistenten angezeigte Komponente **[USB Redirection (USB-Umleitung)]** deaktivieren.
- Wenn Sie die Komponente **[USB Redirection (USB-Umleitung)]** installieren möchten, stellen Sie sicher, dass die Funktion für automatische Windows-Updates auf dem Clientcomputer nicht deaktiviert wurde.
- Legen Sie fest, ob Sie die SSO-Funktion (Single Sign-On) verwenden möchten. Mit dieser Funktion können Endbenutzer sich an View Client und an ihrem virtuellen Desktop als aktuell angemeldeter Benutzer anmelden. Die Anmeldeinformationen des Benutzers, die dieser zur Anmeldung am Clientsystem eingegeben hat, werden an die View Connection Server-Instanz und schließlich an den virtuellen Desktop übergeben. Einige Clientbetriebssysteme bieten keine Unterstützung für diese Funktion.
- Wenn Sie nicht möchten, dass die Endbenutzer die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) der View Connection Server-Instanz eingeben müssen, die ihre virtuelle Maschine hostet, ermitteln Sie die IP-Adresse oder den FQDN, um sie bzw. ihn während der Installation anzugeben.

Vorgehensweise

1 Melden Sie sich als Benutzer mit Administratorberechtigungen am Clientsystem an.

2 Laden Sie die View Client-Installationsdatei von der VMware-Produktseite unter http://www.vmware.com/de/products/ auf das Clientsystem herunter.

Wählen Sie die geeignete Installationsdatei, wobei *xxxxxx* für die Build-Nummer steht.

Option	Aktion
View Client auf 64-Bit-Betriebssystemen	Wählen Sie die Datei `VMware-viewclient-x86_64-4.5.x-xxxxxx.exe` für View Client. Wählen Sie die Datei `VMware-viewclientwithlocalmode-x86_64-4.5.x-xxxxxx.exe` für View Client with Local Mode.
View Client auf 32-Bit-Betriebssystemen	Wählen Sie die Datei `VMware-viewclient-4.5.x-xxxxxx.exe` für View Client. Wählen Sie die Datei `VMware-viewclientwithlocalmode-4.5.x-xxxxxx.exe` für View Client with Local Mode.

3 Zum Starten des View Client-Installationsprogramms doppelklicken Sie auf die Installationsdatei.

4 Folgen Sie den Anweisungen zum Installieren der gewünschten Komponenten.

Der VMware View Client-Dienst wird auf dem Windows-Clientcomputer installiert. Der Dienstname für View Client lautet `wsnm.exe`. Der Dienstname für die USB-Komponente lautet `wsnm_usbctrl.exe`.

Weiter

Starten Sie View Client und stellen Sie sicher, dass Sie sich am richtigen virtuellen Desktop anmelden können. Siehe „Starten von View Client (Windows-basiert) oder View Client with Local Mode“, auf Seite 101 oder „Installieren von View Client unter Verwendung von View Portal“, auf Seite 103.

Starten von View Client (Windows-basiert) oder View Client with Local Mode

Bevor Sie den Endbenutzern Zugriff auf ihre virtuellen Desktops gewähren, sollten Sie sicherstellen, dass Sie sich von einem Clientgerät aus an einem virtuellen Desktop anmelden können. Sie können View Client über das Menü **[Start]** oder eine Desktop-Verknüpfung auf dem Clientsystem starten.

In Umgebungen, in denen eine Netzwerkverbindung verfügbar ist, wird die Benutzersitzung von View Connection Server authentifiziert.

Voraussetzungen

- Stellen Sie sicher, dass View Client oder View Client with Local Mode auf dem Clientgerät installiert ist.
- Wenn Sie View Client with Local Mode verwenden möchten, stellen Sie sicher, dass Ihre Lizenz View Client with Local Mode umfasst und dass der View-Desktop die Anforderungen für den lokalen Modus erfüllt. Weitere Informationen zum Einrichten einer Bereitstellung lokaler Desktops finden Sie in der Themenübersicht im *VMware View-Administratorhandbuch*.
- Stellen Sie sicher, dass ein virtueller Desktop-Pool erstellt wurde und das zu verwendende Benutzerkonto für den Zugriff auf diesen Desktop berechtigt ist. Weitere Informationen finden Sie in den Themen zur Erstellung von Desktop-Pools im *VMware View-Administratorhandbuch*.
- Stellen Sie sicher, dass Sie über den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse der View Connection Server-Instanz verfügen, die Zugriff auf diesen virtuellen Desktop gewährt.

Vorgehensweise

1. Wenn View Client nach der Installation nicht automatisch gestartet wird, doppelklicken Sie auf die Desktop-Verknüpfung oder klicken Sie auf **[Start]** > **[Programs (Programme)]** > **[VMware]** > **[VMware View Client]** .
2. Geben Sie im Dropdown-Menü **[Connection Server]** entweder den Hostnamen oder die IP-Adresse für View Connection Server ein.
3. Stellen Sie sicher, dass die weiteren optionalen Einstellungen im Dialogfeld Ihrer Konfiguration entsprechen.

Option	Beschreibung
Log in as current user (Anmelden als aktueller Benutzer)	Dieses Kontrollkästchen wird gemäß der globalen Einstellung in View Administrator angezeigt oder ausgeblendet. Aktivieren Sie dieses Kontrollkästchen nicht, wenn Sie den View-Desktop für die Verwendung im lokalen Modus auschecken möchten.
Use secure connection (SSL) (Sichere Verbindung verwenden (SSL))	Wenn dieses Kontrollkästchen aktiviert ist, müssen Sie auch die globale Einstellung **[Use SSL for client connections (SSL für Clientverbindungen verwenden)]** in View Administrator auswählen.
Port	Wenn Sie eine sichere Verbindung verwenden, lautet der Standardport 443.
Autoconnect (Automatische Verbindungsherstellung)	Wenn Sie dieses Kontrollkästchen aktivieren, ist das Feld **[Connection Server]** beim nächsten Start von View Client deaktiviert und Sie werden mit dem Server verbunden, den Sie bei Aktivierung des Kontrollkästchens **[Autoconnect (Automatische Verbindungsherstellung)]** angegeben haben. Zur Deaktivierung dieses Kontrollkästchens schließen Sie das nächste Dialogfeld und klicken Sie auf **[Options (Optionen)]** , um diese Einstellung anzuzeigen und zu ändern.

4 Klicken Sie auf **[Connect (Verbinden)]** .

5 Geben Sie die Anmeldeinformationen eines Benutzers ein, der für die Verwendung von mindestens einem Desktop-Pool berechtigt ist, wählen Sie die Domäne aus und klicken Sie auf **[Login (Anmelden)]** .

   Wenn Sie den Benutzernamen mit dem Format **`Benutzer@Domaene`** eingeben, wird er aufgrund des At-Zeichens (@) als Benutzerprinzipalname (User Principal Name, UPN) behandelt, und das Dropdown-Menü für die Domäne wird abgeblendet dargestellt.

   Weitere Informationen zur Erstellung von Desktop-Pools und zum Zuweisen von Benutzerberechtigungen für Pools finden Sie im *VMware View-Administratorhandbuch*.

6 (Optional) Wählen Sie im Dropdown-Menü **[Display (Anzeige)]** die Fenstergröße für die Anzeige des View-Desktops.

7 (Optional) Zur Auswahl eines Anzeigeprotokolls klicken Sie auf den nach unten weisenden Pfeil neben einem Desktop in der Liste, klicken Sie auf **[Display Protocol (Anzeigeprotokoll)]** und wählen Sie das gewünschte Protokoll.

   Diese Auswahl ist nur verfügbar, wenn sie durch View Administrator aktiviert wurde.

8 Wählen Sie einen Desktop aus der Liste der Desktop-Pools und klicken Sie auf **[Connect (Verbinden)]** .

   View Client versucht, eine Verbindung mit einem Desktop im angegebenen Pool herzustellen.

Nachdem die Verbindung hergestellt wurde, wird das Clientfenster angezeigt.

Wenn keine Authentifizierung gegenüber View Connection Server möglich ist oder View Client keine Verbindung mit einem Desktop herstellen kann, führen Sie die folgenden Aufgaben aus:

- Stellen Sie sicher, dass die View Client-Einstellung für die Verwendung sicherer Verbindungen (SSL) der globalen Einstellung in View Administrator entspricht. Wenn das Kontrollkästchen für sichere Verbindungen z.B. auf dem Client deaktiviert ist, muss das Kontrollkästchen auch in View Administrator deaktiviert sein.
- Stellen Sie eine ordnungsgemäße Funktionsweise des Sicherheitszertifikats für View Connection Server sicher. Wenn dies nicht zutrifft, wird in View Administrator möglicherweise angezeigt, dass View Agent in Desktops nicht erreichbar ist, und über den Transfer Server-Status wird angezeigt, dass die Komponente nicht bereit ist. Dies sind Hinweise auf zusätzliche Verbindungsprobleme, die durch Zertifikatprobleme verursacht werden.
- Stellen Sie sicher, dass die für die View Connection Server-Instanz festgelegten Kennzeichen Verbindungen von diesem Benutzer erlauben. Weitere Informationen finden Sie im *VMware View-Administratorhandbuch*.
- Stellen Sie sicher, dass der Benutzer zum Zugriff auf diesen Desktop berechtigt ist. Weitere Informationen finden Sie im *VMware View-Administratorhandbuch*.
- Stellen Sie sicher, dass der Clientcomputer Remote-Desktop-Verbindungen zulässt.

Weiter

- Konfigurieren Sie Startoptionen.

  Wenn Sie nicht möchten, dass Endbenutzer den Hostnamen oder die IP-Adresse von View Connection Server eingeben müssen, oder wenn Sie andere Startoptionen konfigurieren möchten, verwenden Sie die View Client-Befehlszeilenoptionen, um eine Desktop-Verknüpfung zu erstellen. Weitere Informationen finden Sie im *VMware View-Administratorhandbuch*.
- Checken Sie einen Desktop aus, der im lokalen Modus verwendet werden kann.

Endbenutzer können feststellen, ob ein Desktop ausgecheckt werden kann, indem sie in der von View Client with Local Mode bereitgestellten Liste auf den nach unten weisenden Pfeil neben dem Desktop klicken. Wenn der Desktop im lokalen Modus verwendet werden kann, wird die Option **[Check out (Auschecken)]** im Kontextmenü angezeigt. Nur der Benutzer, der den Desktop auscheckt, kann auf den Desktop zugreifen. Dies gilt selbst dann, wenn einer Gruppe von Benutzern Berechtigungen für den Desktop erteilt wurden.

Installieren von View Client unter Verwendung von View Portal

Eine bequeme Methode zum Installieren von View Client oder View Client with Local Mode besteht darin, einen Browser zu öffnen und zur View Portal-Webseite zu wechseln. Sie können über View Portal das vollständige Installationsprogramm für View Client herunterladen, sowohl für Windows- als auch für Mac-Clientcomputer.

Ab View 4.5 installiert View Portal den vollständigen View Client für Windows, mit oder ohne den lokalen Modus, sowie View Client für Mac.

HINWEIS View Portal bietet keine Unterstützung für Linux. Für Linux wird ein nativer Client nur über zertifizierte VMware-Partner zur Verfügung gestellt.

Voraussetzungen

- Stellen Sie sicher, dass Sie über die URL für die View Connection Server-Instanz verfügen.
- Stellen Sie sicher, dass Sie sich als Administrator auf dem Clientsystem anmelden können.
- Stellen Sie sicher, dass ein virtueller Desktop erstellt wurde und dass das zu verwendende Benutzerkonto für zum Zugriff auf diesen Desktop berechtigt ist.
- Stellen Sie sicher, dass das Clientsystem ein unterstütztes Betriebssystem verwendet. Siehe „Unterstützte Betriebssysteme für View Client und View Client with Local Mode“, auf Seite 16.
- Stellen Sie sicher, dass View Agent nicht installiert ist.
- Wenn Sie View Client with Local Mode installieren möchten, stellen Sie sicher, dass Ihre Lizenz View Client with Local Mode umfasst.
- Wenn Sie View Client with Local Mode installieren möchten, stellen Sie sicher, dass keins der folgenden Produkte installiert ist: VMware View Client, VMware Player, VMware Workstation, VMware ACE, VMware Server.
- Bestimmen Sie, ob der Benutzer des Clientgeräts von einem virtuellen Desktop auf lokal angeschlossene USB-Geräte zugreifen darf. Falls nicht, müssen Sie die vom Assistenten angezeigte Komponente **[USB Redirection (USB-Umleitung)]** deaktivieren.
- Wenn Sie die Komponente **[USB Redirection (USB-Umleitung)]** installieren möchten, stellen Sie sicher, dass die Funktion für automatische Windows-Updates auf dem Clientcomputer nicht deaktiviert wurde.

Vorgehensweise

1. Melden Sie sich als Benutzer mit Administratorberechtigungen am Clientsystem an.
2. Öffnen Sie einen Browser und geben Sie die URL der View Connection Server-Instanz ein, die Zugriff auf den virtuellen Desktop bietet.

   Internet Explorer kann ermitteln, ob ein Upgrade verfügbar ist. Bei Firefox und Safari ist dies nicht möglich. Darüber hinaus zeigt Internet Explorer in der Liste der Installationsprogramme 32-Bit-Installationsprogramme an, wenn der Client über ein 32-Bit-Betriebssystem verfügt, und 64-Bit-Installationsprogramme, wenn der Client über ein 64-Bit-Betriebssystem verfügt. Bei Firefox werden sowohl 32-Bit- als auch 64-Bit-Installationsprogramme aufgeführt.

3 Folgen Sie den Anweisungen auf der Webseite.

Falls die verfügbare Version von View Connection Server neuer ist als die auf dem Clientgerät installierte Version, können Sie ein Upgrade durchführen. Wenn die Version mit der auf dem Clientgerät übereinstimmt, startet View Portal den auf dem Clientcomputer installierten View Client.

Wenn Sie über eine ältere Version von View Client verfügen und für Clientverbindungen eine Smartcard erforderlich ist, werden Sie in Internet Explorer aufgefordert, Ihre Smartcard einzulegen, bevor View Portal die vorhandene View Client-Version überprüft.

4 Wenn Internet Explorer Sie zum Einlegen einer Smartcard auffordert, legen Sie entweder die Karte ein oder klicken Sie auf **[Cancel (Abbrechen)]** .

Das Einlegen einer Smartcard und das Klicken auf **[Cancel (Abbrechen)]** haben die gleiche Wirkung.

Weiter

Stellen Sie eine Verbindung mit dem View-Desktop her. Siehe „Starten von View Client (Windows-basiert) oder View Client with Local Mode“, auf Seite 101 oder „Starten von View Client unter Mac OS X“, auf Seite 105.

Installieren von View Client auf Mac OS X

Endbenutzer öffnen View Client, um von einem physischen Mac OS X-Computer eine Verbindung mit virtuellen Desktops herzustellen. View Client wird auf Mac OS X-Clientsystemen über eine Festplatten-Image-Datei installiert.

Voraussetzungen

- Stellen Sie sicher, dass das Clientsystem ein unterstütztes Betriebssystem verwendet. Siehe „Unterstützte Betriebssysteme für View Client und View Client with Local Mode“, auf Seite 16.
- Stellen Sie sicher, dass das Mac-Clientsystem über Remotedesktopverbindung 2.0 oder höher verfügt. Die Festplatten-Image-Datei von View Client umfasst einen Link zur Downloadseite für den Microsoft-Remotedesktopverbindungs-Client für Mac.

Vorgehensweise

1 Melden Sie sich am Clientsystem an.

2 Laden Sie auf dem Clientsystem die Festplatten-Image-Datei für View Client von der VMware-Produktseite unter http://www.vmware.com/de/products/ herunter.

Wählen Sie die Festplatten-Image-Datei `VMware-View-Client-4.5.`*`x`*`-`*`xxxxxx`*`.dmg`, wobei *xxxxxx* für die Build-Nummer steht.

3 Doppelklicken Sie auf die `.dmg`-Datei, um diese zu öffnen, und anschließend auf **[Agree (Zustimmen)]** .

Die Inhalte des Festplatten-Images werden in einem Finder-Fenster für VMware View Client angezeigt.

4 Öffnen Sie ein neues Finder-Fenster und navigieren Sie zum Ordner **[Applications (Programme)]** .

5 Ziehen Sie das VMware View Client-Symbol in den Ordner **[Applications (Programme)]** .

Wenn Sie nicht als Administrator angemeldet sind, werden Sie aufgefordert, einen Administratorbenutzernamen und ein Kennwort einzugeben.

Sie können das Festplatten-Image jetzt unmounten.

Weiter

Starten Sie View Client und stellen Sie sicher, dass Sie sich am richtigen virtuellen Desktop anmelden können. Siehe „Starten von View Client unter Mac OS X“, auf Seite 105.

Starten von View Client unter Mac OS X

Bevor Endbenutzer auf ihre virtuellen Desktops zugreifen, sollten Sie testen, ob Sie sich über ein Mac-Clientsystem an einem virtuellen Desktop anmelden können.

Neben dem Zugriff auf virtuelle Desktops bietet View Client die Möglichkeit, Einstellungen zu konfigurieren. Beispielsweise können Endbenutzer eine Fenstergröße auswählen oder ihre aktuellen Anmeldeinformationen für die View-Authentifizierung verwenden.

Voraussetzungen

- Stellen Sie sicher, dass View Client auf dem Clientsystem installiert ist.
- Stellen Sie sicher, dass ein virtueller Desktop-Pool erstellt wurde und das zu verwendende Benutzerkonto für den Zugriff auf diesen Desktop berechtigt ist. Weitere Informationen finden Sie in den Themen zur Erstellung von Desktop-Pools im *VMware View-Administratorhandbuch*.
- Stellen Sie sicher, dass Sie über den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse der View Connection Server-Instanz verfügen, die Zugriff auf diesen virtuellen Desktop gewährt.
- Stellen Sie sicher, dass die View Agent-Gruppenrichtlinieneinstellung **[AllowDirectRDP (Direkte RDP-Verbindung zulassen)]** aktiviert ist. Diese Einstellung ist standardmäßig aktiviert.

Vorgehensweise

1. Doppelklicken Sie im Installationsordner von View Client (normalerweise der Ordner **[Applications (Programme)]**) auf **[VMware View Client]** .
2. Wählen Sie im Dropdown-Menü **[Address (Adresse)]** Ihre View Connection Server-Instanz aus oder geben Sie den Hostnamen oder die IP-Adresse des Servers ein.
3. (Optional) Wählen Sie die Optionen für die Art der Verbindung mit dem ausgewählten Server aus.

Option	Beschreibung
Port	Geben Sie die Portnummer an oder lassen Sie das Feld leer, um den Standardport für die View Connection Server-Instanz zu verwenden.
Use Secure Connection (SSL) (Sichere Verbindung verwenden (SSL))	Wählen Sie diese Option zur Verwendung einer sicheren Verbindung (SSL), um vertrauliche Unternehmensdaten zu schützen und um sicherzustellen, dass alle Verbindungen vollständig verschlüsselt werden. Ihr View-Administrator hat View Connection Server möglicherweise so konfiguriert, dass selbst bei Auswahl einer nicht sicheren Verbindung durch den Benutzer eine sichere Verbindung verwendet wird.
Always connect to this server at startup (Beim Start immer mit diesem Server verbinden)	Wählen Sie diese Option, um beim Start von View Client direkt eine Verbindung mit der aktuellen View Connection Server-Instanz herzustellen. Wählen Sie diese Option, wenn Sie immer eine Verbindung mit derselben View Connection Server-Instanz herstellen. Bei Deaktivierung dieser Option muss beim Start von View Client eine View Connection Server-Instanz eingegeben oder ausgewählt werden.

   Sie können den Port und die SSL-Optionen auch direkt über das Adressfeld eingeben. Für eine Verbindung ohne SSL geben Sie **`http://<URL>[:Portnummer]`** ein. Für eine SSL-Verbindung geben Sie **`http://<URL>[:Portnummer]`** ein.

4. Klicken Sie auf **[Continue (Fortfahren)]** .

   Sie sind mit View Connection Server verbunden und können sich jetzt anmelden.

5. Geben Sie im Anmeldedialogfenster Ihren Benutzernamen und Ihr Kennwort ein.

   Bei Eingabe des Benutzernamens in der Form **`benutzer@domaene`** wird dieser aufgrund des At-Zeichens (**`@`**) als Benutzerprinzipalname behandelt, sodass das Dropdown-Menü für die Domäne abgeblendet angezeigt wird. Anderenfalls muss auch eine Domäne ausgewählt werden.

6 (Optional) Wählen Sie **[Remember this password in my keychain (Kennwort im Schlüsselbund sichern)]** , um Ihre Anmeldeinformationen sicher zu speichern.

7 Klicken Sie auf **[Continue (Fortfahren)]** .

Bei erfolgreicher Anmeldung wird die Liste der Desktops angezeigt, für deren Verwendung Sie berechtigt sind.

8 Wählen Sie einen Desktop aus der Liste aus.

9 (Optional) Wählen Sie eine Option aus dem Dropdown-Menü **[Display (Anzeige)]** aus.

Option	Beschreibung
Full Screen (Vollbild)	Zeigt den Desktop auf dem gesamten Bildschirm an. Wenn Sie den Vollbildmodus wählen und über mehrere Bildschirme verfügen, ziehen Sie das Fenster für die Desktop-Auswahl auf den Bildschirm, auf dem der Desktop angezeigt werden soll.
Large Window (Großes Fenster)	Zeigt den Desktop in einem großen Fenster an.
Small Window (Kleines Fenster)	Zeigt den Desktop in einem kleinen Fenster an.
Custom (Benutzerdefiniert)	Legen Sie mithilfe des Schiebereglers im angezeigten Dialogfeld die Fenstergröße fest und klicken Sie auf **[Select (Auswählen)]** . Die ausgewählte Größe wird zum Dropdown-Menü **[Display (Anzeige)]** hinzugefügt.

Anzeigeeinstellungen werden beim nächsten Öffnen des Desktops beibehalten.

10 Klicken Sie auf **[Continue (Fortfahren)]** oder wählen Sie im Menü **[Action (Aktion)]** (das Menü mit dem Zahnradsymbol) die Option **[Connect (Verbinden)]** .

Nachdem die Verbindung hergestellt wurde, wird das Clientfenster angezeigt. Wenn View Client keine Verbindung mit dem Desktop herstellen kann, führen Sie die folgenden Aufgaben aus:

- Stellen Sie sicher, dass die View Client-Einstellung für die Verwendung sicherer Verbindungen (SSL) der globalen Einstellung in View Administrator entspricht. Wenn das Kontrollkästchen für sichere Verbindungen z.B. auf dem Client deaktiviert ist, muss das Kontrollkästchen auch in View Administrator deaktiviert sein.
- Stellen Sie eine ordnungsgemäße Funktionsweise des Sicherheitszertifikats für View Connection Server sicher. Wenn dies nicht zutrifft, wird in View Administrator möglicherweise angezeigt, dass View Agent in Desktops nicht erreichbar ist.
- Stellen Sie sicher, dass die für die View Connection Server-Instanz festgelegten Kennzeichen Verbindungen von diesem Benutzer erlauben. Weitere Informationen finden Sie im *VMware View-Administratorhandbuch*.
- Stellen Sie sicher, dass der Benutzer zum Zugriff auf diesen Desktop berechtigt ist. Weitere Informationen finden Sie im *VMware View-Administratorhandbuch*.
- Stellen Sie sicher, dass der Clientcomputer Remote-Desktop-Verbindungen zulässt.

Weiter

Anweisungen zur Verwendung von View Client finden Sie in der Hilfe zu VMware View Client.

Festlegen von Voreinstellungen für die virtuelle Druckfunktion

Die virtuelle Druckfunktion ermöglicht Endbenutzern das Verwenden von lokalen oder Netzwerkdruckern auf einem View-Desktop, ohne dass im View-Desktop zusätzliche Druckertreiber installiert werden müssen. Für jeden Drucker, der über diese Funktion zur Verfügung steht, können Sie Voreinstellungen für Datenkomprimierung, Druckqualität, doppelseitigen Druck, Farbe usw. festlegen.

Wenn dem lokalen Computer ein Drucker hinzugefügt wird, fügt View diesen Drucker zur Liste der verfügbaren Drucker auf dem View-Desktop hinzu. Es ist keine weitere Konfiguration erforderlich. Benutzer mit Administratorrechten können weiterhin Druckertreiber auf dem View-Desktop installieren, ohne einen Konflikt mit der virtuellen Druckfunktion zu verursachen.

Wichtig Diese Funktion steht für die folgenden Druckertypen nicht zur Verfügung:

- USB-Drucker, die die USB-Umleitungsfunktion zur Verbindung mit einem virtuellen USB-Port im View-Desktop verwenden

  Sie müssen den USB-Drucker im View-Desktop trennen, um die virtuelle Druckfunktion verwenden zu können.

- Die Windows-Funktion für die Ausgabe in einer Datei

  Das Kontrollkästchen **[Print to file (Ausgabe in Datei)]** im Dialogfeld **[Print (Drucken)]** kann nicht ausgewählt werden. Ein Druckertreiber, über den eine Datei erstellt wird, kann verwendet werden. Beispielsweise können Sie einen PDF-Writer zum Drucken einer PDF-Datei verwenden.

Voraussetzungen

Stellen Sie sicher, dass die virtuelle Druckfunktion von View Agent auf dem View-Desktop installiert ist. Die Treiber befinden sich im View-Desktop-Dateisystem unter `C:\Programme\Gemeinsame Dateien\VMware\Drivers\Virtual Printer`.

Die Installation von View Agent ist eine der Aufgaben, die im Rahmen der Vorbereitung einer virtuellen Maschine auf die Verwendung als View-Desktop durchgeführt werden muss. Weitere Informationen finden Sie im *VMware View-Administratorhandbuch*.

Vorgehensweise

1. Klicken Sie im View-Desktop auf **[Start] > [Settings (Einstellungen)] > [Printers and Faxes (Drucker und Faxgeräte)]** .
2. Klicken Sie im Fenster **[Printers and Faxes (Drucker und Faxgeräte)]** mit der rechten Maustaste auf einen der lokal verfügbaren Drucker und wählen Sie **[Properties (Eigenschaften)]** .

   Auf Windows 7-Desktops wird möglicherweise nur der Standarddrucker angezeigt, selbst wenn weitere Drucker verfügbar sind. Zum Anzeigen der anderen Drucker klicken Sie mit der rechten Maustaste auf den Standarddrucker und zeigen auf **[Printer Properties (Druckeigenschaften)]** .
3. Klicken Sie im Fenster mit den Druckeigenschaften auf die Registerkarte **[ThinPrint Device Setup (ThinPrint-Geräteeinrichtung)]** und geben Sie die zu verwendenden Einstellungen an.
4. Klicken Sie auf der Registerkarte **[General (Allgemein)]** auf **[Printing Preferences (Druckeinstellungen)]** und bearbeiten Sie die Seiten- und Farbeinstellungen.
5. Auf der Registerkarte **[Advanced (Erweitert)]** legen Sie die Einstellungen für den doppelseitigen Druck und das Druckformat (Hochformat oder Querformat) fest.
6. Zur Anzeige einer Druckvorschau auf dem Host aktivieren Sie **[Preview on client before printing (Vor dem Druck Vorschau auf Client anzeigen)]** .

   Aus dieser Vorschau können Sie auf einen beliebigen Drucker mit allen verfügbaren Eigenschaften zugreifen.

7 Auf der Registerkarte **[Adjustment (Anpassung)]** können Sie die Optionen für die automatische Druckanpassung überprüfen.

VMware empfiehlt die Beibehaltung der Standardeinstellungen.

8 Klicken Sie auf **[OK]** .

Verwenden von USB-Druckern

In einer View-Umgebung können virtuelle Drucker und umgeleitete USB-Drucker konfliktfrei zusammen eingesetzt werden.

Ein USB-Drucker ist ein Drucker, der über einen USB-Port an das lokale Clientsystem angeschlossen ist. Um Druckaufträge an einen USB-Drucker zu senden, können Sie entweder die USB-Umleitungsfunktion oder die virtuelle Druckfunktion verwenden.

- Sie können die USB-Umleitungsfunktion verwenden, um einen USB-Drucker über einen virtuellen USB-Port an den View-Desktop anzuschließen, wenn die erforderlichen Treiber ebenfalls auf dem View-Desktop installiert sind.

  Bei Verwendung dieser Umleitungsfunktion ist der Drucker nicht mehr mit dem physischen USB-Port am Client verbunden, sodass der USB-Drucker nicht in der Liste der lokalen Drucker aufgeführt wird, die über die virtuelle Druckfunktion angezeigt wird. Dies bedeutet auch, dass Sie vom View-Desktop auf dem USB-Drucker drucken können, jedoch nicht von der lokalen Clientmaschine.

- Alternativ können Sie die virtuelle Druckfunktion verwenden, um Druckaufträge an einen USB-Drucker zu senden. Bei Verwendung der virtuellen Druckfunktion können Sie sowohl vom View-Desktop als auch vom lokalen Client auf dem USB-Drucker drucken, ohne Druckertreiber im View-Desktop installieren zu müssen.

Unbeaufsichtigte Installation von View Client

Sie können eine unbeaufsichtigte Installation von View Client durchführen, indem Sie den Namen der Installationsdatei sowie die gewünschten Installationsoptionen an der Befehlszeile eingeben. Die unbeaufsichtigte Installation ermöglicht eine effiziente Bereitstellung von View-Komponenten in einem großen Unternehmen.

Festlegen von Gruppenrichtlinien zum Zulassen einer unbeaufsichtigten Installation von View Client with Local Mode

Bevor Sie eine unbeaufsichtigte Installation von View Client with Local Mode ausführen können, müssen Sie Microsoft Windows-Gruppenrichtlinien konfigurieren, um eine Installation mit erhöhten Rechten zuzulassen.

Zur unbeaufsichtigten Installation von View Client ist das Festlegen dieser Gruppenrichtlinien nicht erforderlich. Diese Richtlinien werden nur für View Client with Local Mode benötigt.

Sie müssen Windows Installer-Gruppenrichtlinien für Computer und Benutzer auf dem Clientcomputer festlegen.

Voraussetzungen

Stellen Sie sicher, dass Sie auf dem Windows-Clientcomputer, auf dem Sie View Client with Local Mode installieren möchten, über Administratorberechtigungen verfügen.

Vorgehensweise

1 Melden Sie sich am Clientcomputer an und klicken Sie auf **[Start] > [Run (Ausführen)]** .

2 Geben Sie **`gpedit.msc`** ein und klicken Sie auf **[OK]** .

3 Klicken Sie im Gruppenrichtlinienobjekt-Editor auf **[Local Computer Policy (Richtlinie für 'Lokaler Computer')] > [Computer Configuration (Computerkonfiguration)]** .

4 Erweitern Sie **[Administrative Templates (Administrative Vorlagen)]**, öffnen Sie den Ordner **[Windows Installer]** und doppelklicken Sie auf **[Always install with elevated privileges (Immer mit erhöhten Rechten installieren)]**.

5 Klicken Sie im Fenster **[Always Install with Elevated Privileges Properties (Eigenschaften von 'Immer mit erhöhten Rechten installieren')]** auf **[Enabled (Aktiviert)]** und anschließend auf **[OK]**.

6 Klicken Sie im linken Fensterbereich auf **[User Configuration (Benutzerkonfiguration)]**.

7 Erweitern Sie **[Administrative Templates (Administrative Vorlagen)]**, öffnen Sie den Ordner **[Windows Installer]** und doppelklicken Sie auf **[Always install with elevated privileges (Immer mit erhöhten Rechten installieren)]**.

8 Klicken Sie im Fenster **[Always Install with Elevated Privileges Properties (Eigenschaften von 'Immer mit erhöhten Rechten installieren')]** auf **[Enabled (Aktiviert)]** und anschließend auf **[OK]**.

Weiter

Führen Sie eine unbeaufsichtigte Installation von View Client with Local Mode aus.

Unbeaufsichtigte Installation von View Client

Sie können die Microsoft Windows Installer-Funktion (MSI) für die unbeaufsichtigte Installation dazu verwenden, View Client oder View Client with Local Mode auf mehreren Windows-Computern zu installieren. Bei einer unbeaufsichtigten Installation verwenden Sie die Befehlszeile und müssen nicht auf Eingabeaufforderungen des Assistenten reagieren.

Voraussetzungen

- Stellen Sie sicher, dass Sie sich als Administrator auf dem Clientsystem anmelden können.
- Stellen Sie sicher, dass das Clientsystem ein unterstütztes Betriebssystem verwendet. Siehe „Unterstützte Betriebssysteme für View Client und View Client with Local Mode“, auf Seite 16.
- Wenn Sie View Client with Local Mode installieren möchten, stellen Sie sicher, dass Ihre Lizenz View Client with Local Mode umfasst.
- Wenn Sie View Client with Local Mode installieren möchten, stellen Sie sicher, dass keins der folgenden Produkte installiert ist: VMware View Client, VMware Player, VMware Workstation, VMware ACE, VMware Server.
- Legen Sie fest, ob Sie die SSO-Funktion (Single Sign-On) verwenden möchten. Mit dieser Funktion können Endbenutzer sich an View Client und an ihrem virtuellen Desktop als aktuell angemeldeter Benutzer anmelden. Die Anmeldeinformationen des Benutzers, die dieser zur Anmeldung am Clientsystem eingegeben hat, werden an die View Connection Server-Instanz und schließlich an den virtuellen Desktop übergeben. Einige Clientbetriebssysteme bieten keine Unterstützung für diese Funktion.
- Wenn Sie nicht möchten, dass die Endbenutzer die IP-Adresse oder den vollqualifizierten Domänennamen (FQDN) der View Connection Server-Instanz eingeben müssen, die ihre virtuelle Maschine hostet, ermitteln Sie die IP-Adresse oder den FQDN, um sie bzw. ihn während der Installation anzugeben.
- Machen Sie sich mit den MSI-Befehlszeilenoptionen vertraut. Siehe „Microsoft Windows Installer-Befehlszeilenoptionen“, auf Seite 54.
- Machen Sie sich mit den verfügbaren MSI-Eigenschaften für die unbeaufsichtigte Installation von View Client vertraut. Siehe „Eigenschaften für die unbeaufsichtigte Installation von View Client“, auf Seite 110.

- Legen Sie fest, ob Sie Endbenutzern von ihren virtuellen Desktops aus den Zugriff auf lokal angeschlossene USB-Geräte gestatten möchten. Falls nicht, legen Sie über die MSI-Eigenschaft `ADDLOCAL` die Liste der relevanten Funktionen fest und lassen Sie die USB-Funktion aus. Weitere Informationen finden Sie unter „Eigenschaften für die unbeaufsichtigte Installation von View Client“, auf Seite 110.
- Wenn Sie View Client with Local Mode installieren, stellen Sie sicher, dass die für die unbeaufsichtigte Installation erforderlichen Windows Installer-Gruppenrichtlinien auf dem Clientcomputer konfiguriert sind. Siehe „Festlegen von Gruppenrichtlinien zum Zulassen einer unbeaufsichtigten Installation von View Client with Local Mode“, auf Seite 108.

Vorgehensweise

1 Laden Sie die View Client-Installationsdatei von der VMware-Produktseite unter http://www.vmware.com/de/products/ auf das Clientsystem herunter.

Wählen Sie die geeignete Installationsdatei, wobei *xxxxxx* für die Build-Nummer steht.

Option	Aktion
View Client auf 64-Bit-Betriebssystemen	Wählen Sie die Datei `VMware-viewclient-x86_64-4.5.x-xxxxxx.exe` für View Client. Wählen Sie die Datei `VMware-viewclientwithlocalmode-x86_64-4.5.x-xxxxxx.exe` für View Client with Local Mode.
View Client auf 32-Bit-Betriebssystemen	Wählen Sie die Datei `VMware-viewclient-4.5.x-xxxxxx.exe` für View Client. Wählen Sie die Datei `VMware-viewclientwithlocalmode-4.5.x-xxxxxx.exe` für View Client with Local Mode.

2 Öffnen Sie auf dem Windows-Clientcomputer eine Eingabeaufforderung.

3 Geben Sie den Installationsbefehl in einer Zeile ein.

Im folgenden Beispiel wird View Client mit SSO (Single Sign-On) und USB-Umleitung installiert. Für die View Client-Benutzer wird eine standardmäßige View Connection Server-Instanz konfiguriert: `VMware-viewclient-4.5.x-xxxxxx.exe /s /v"/qn VDM_SERVER=cs1.companydomain.com ADDLOCAL=Core,TSSO,USB"`

In diesem Beispiel wird View Client with Local Mode installiert: `VMware-viewclientwithlocal-4.5.x-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,MVDI"`

Hinweis Die Funktion `Core` ist verbindlich.

Der VMware View Client-Dienst wird auf dem Windows-Clientcomputer installiert.

Weiter

Starten Sie View Client und stellen Sie sicher, dass Sie sich am richtigen virtuellen Desktop anmelden können. Siehe „Starten von View Client (Windows-basiert) oder View Client with Local Mode“, auf Seite 101 oder „Installieren von View Client unter Verwendung von View Portal“, auf Seite 103.

Eigenschaften für die unbeaufsichtigte Installation von View Client

Sie können spezielle Eigenschaften einschließen, wenn Sie eine unbeaufsichtigte Installation von View Client über die Befehlszeile ausführen. Sie müssen hierbei das Format *`EIGENSCHAFT=Wert`* einhalten, damit Microsoft Windows Installer (MSI) die Eigenschaften und Werte interpretieren kann.

Tabelle 9-1 zeigt die Eigenschaften für eine unbeaufsichtigte Installation von View Client, die Sie an der Befehlszeile verwenden können.

Tabelle 9-1. MSI-Eigenschaften für die unbeaufsichtigte Installation von View Client

MSI-Eigenschaft	Beschreibung	Standardwert
INSTALLDIR	Der Pfad und der Ordner, in dem die View Client-Software installiert wird. Beispiel: `INSTALLDIR=""D:\abc\Mein Ordner""` Die zweifach gesetzten doppelten Anführungszeichen um den Pfad sorgen dafür, dass das MSI-Installationsprogramm das Leerzeichen im Pfad ignoriert. Diese MSI-Eigenschaft ist optional.	`%ProgramFiles% \VMware, Inc. \VMware View Client`
VDM_SERVER	Der vollqualifizierte Domänenname (FQDN) oder die IP-Adresse der View Connection Server-Instanz, mit der View Client-Benutzer standardmäßig eine Verbindung herstellen. Wenn Sie diese Eigenschaft konfigurieren, müssen View Client-Benutzer diesen FQDN bzw. die IP-Adresse nicht angeben. Beispiel: `VDM_SERVER=cs1.companydomain.com` Diese MSI-Eigenschaft ist optional.	–
DESKTOP_SHORTCUT	Konfiguriert eine Desktop-Verknüpfung für View Client. Bei Verwendung des Werts 1 wird eine Verknüpfung erstellt. Bei Verwendung des Werts 0 wird keine Verknüpfung erstellt. Diese MSI-Eigenschaft ist optional.	1
QUICKLAUNCH_SHORTCUT	Konfiguriert ein Verknüpfungssymbol für View Client in der Schnellstartleiste. Bei Verwendung des Werts 1 wird eine Verknüpfung erstellt. Bei Verwendung des Werts 0 wird keine Verknüpfung erstellt. Diese MSI-Eigenschaft ist optional.	1
STARTMENU_SHORTCUT	Konfiguriert eine Verknüpfung für View Client im Startmenü. Bei Verwendung des Werts 1 wird eine Verknüpfung erstellt. Bei Verwendung des Werts 0 wird keine Verknüpfung erstellt. Diese MSI-Eigenschaft ist optional.	1

In einem Befehl für die unbeaufsichtigte Installation können Sie mit der MSI-Eigenschaft `ADDLOCAL=` Funktionen angeben, die das View Client-Installationsprogramm konfiguriert. Jede Funktion für die unbeaufsichtigte Installation entspricht einer Setup-Option, die Sie während einer interaktiven Installation auswählen können.

Tabelle 9-2 zeigt die View Client-Funktionen, die Sie an der Befehlszeile angeben können, sowie die entsprechenden Optionen in einer interaktiven Installation.

Tabelle 9-2. Funktionen für die unbeaufsichtigte View Client-Installation und benutzerdefinierte Setup-Optionen bei einer interaktiven Installation

Funktion für die unbeaufsichtigte Installation	Benutzerdefinierte Setup-Option bei einer interaktiven Installation
Core Wenn Sie mithilfe der MSI-Eigenschaft `ADDLOCAL=` einzelne Funktionen angeben, müssen Sie **`Core`** einschließen. Bei Verwendung der Eigenschaft `ADDLOCAL=ALL` werden alle Funktionen für View Client und View Client with Local Mode, einschließlich Core, installiert.	– Bei einer interaktiven Installation werden die View Client-Hauptfunktionen standardmäßig installiert.
MVDI Verwenden Sie diese Funktion, wenn Sie View Client with Local Mode installieren und mit `ADDLOCAL=` einzelne Funktionen angeben. Bei Verwendung der Eigenschaft `ADDLOCAL=ALL` werden alle Funktionen für View Client with Local Mode, einschließlich MVDI, installiert.	– Wenn Sie View Client with Local Mode interaktiv installieren, werden die MVDI-Funktionen standardmäßig installiert. Wenn Sie View Client interaktiv installieren, stehen die MVDI-Funktionen nicht zur Verfügung.
ThinPrint	Virtuelle Druckfunktion

Tabelle 9-2. Funktionen für die unbeaufsichtigte View Client-Installation und benutzerdefinierte Setup-Optionen bei einer interaktiven Installation (Fortsetzung)

Funktion für die unbeaufsichtigte Installation	Benutzerdefinierte Setup-Option bei einer interaktiven Installation
TSSO	Einmalige Anmeldung (Single Sign-On, SSO)
USB	USB-Umleitung

Index

A

Active Directory
- Konfigurieren von Domänen und Vertrauensbeziehungen **23**
- Vorbereitung für Smartcard-Authentifizierung **27**
- Vorbereitung zur Verwendung mit View **23**

Active Directory-Gruppen
- Erstellung für Clientkonten im Kiosk-Modus **24**
- Erstellung für View-Benutzer und Administratoren **25**

ADM-Vorlagendateien **26**

Adobe Flash-Anforderungen **22**

Anmelden als aktueller Benutzer **101**

Antivirensoftware, View Composer **40**

Anzeigeanforderungen, Desktops im lokalen Modus **16**

Arbeitsblätter, Berechnen der Anzahl kurzlebiger Ports und der Größe der TCB-Hash-Tabelle **71**

Arbeitsspeicheranforderungen, Desktops im lokalen Modus **16**

Auslagerungsdatei, Größe, View Connection Server **73**

B

Benutzerkonten
- Anforderungen **56**
- vCenter Server **25, 56**
- View Composer **25, 56**

Browseranforderungen **9, 18**

C

Certificate Signing Request (CSR), *siehe* CSR-Anfrage

certutil, Befehl **29**

Clientsoftwareanforderungen **15**

CPU-Anforderungen, Desktops im lokalen Modus **16**

CSR-Anfrage, erstellen **89**

D

Datenbanken
- Erstellung für View Composer **31**
- View-Ereignisse **95, 97**

Deinstallieren von View-Komponenten **55**

Direkte Verbindungen, konfigurieren **65**

DNS-Auflösung, View Composer **40**

Dokumentationsfeedback, Vorgehensweise **5**

Domänenfilterung **24**

Drucker, einrichten **107**

E

Eingeschränkte Gruppen, Richtlinie, konfigurieren **26**

Enterprise NTAuth-Speicher, Hinzufügen von Stammzertifikaten **29**

Ereignisdatenbank
- Erstellung für View **95, 97**
- SQL Server-Konfiguration **96**

ESX-Hosts, View Composer **39**

externe URLs, Zweck und Format **65**

Externe URLs
- Ändern für einen Sicherheitsserver **66**
- konfigurieren, für View Connection Server-Instanz **66**

F

Firefox, unterstützte Versionen **9, 18**

Firewall-Regeln
- View Connection Server **45**
- View Transfer Server **80**

Firewalls, konfigurieren **42**

G

Glossar, Speicherort **5**

GPOs, Verknüpfung mit einer View-Desktop-OU **26**

Größeneinstellungen für Windows Server
- Arbeitsblätter zur Berechnung **71**
- Berechnen der Anzahl kurzlebiger Ports **67**
- Erhöhen der Anzahl kurzlebiger Ports **67, 68**
- Vergrößern der TCB-Hash-Tabelle **70**
- Vergrößern des JVM-Heaps **72**

GroupPolicyFiles, Verzeichnis **26**

Gruppenrichtlinienobjekte, *siehe* GPOs

H

Hardwareanforderungen
- Desktops im lokalen Modus **16**
- PCoIP **19**
- Smartcard-Authentifizierung **22**

HP RGS **21**

I

Internet Explorer, unterstützte Versionen **9, 18**

J

JVM-Heap-Größe
- Standardeinstellung **72**
- vergrößern **72**

K

keyfile, Eigenschaft **91**

keypass, Eigenschaft **91**

keytool, Dienstprogramm
- Erstellen einer CSR-Anfrage **89**
- Generieren einer Schlüsselspeicherdatei **88**
- Hinzufügen zum Systempfad **86**

Kiosk-Modus, Active Directory-Vorbereitung **24**

Kurzlebige Ports
- berechnen **67**
- Erhöhen der Anzahl auf einem Windows Server-Computer **68**
- Verwendung durch View Manager **67**

L

Lizenzschlüssel, View Connection Server **61**

locked.properties, Datei **91**

Lokale Desktops, Konfiguration
- Berechtigungen für vCenter Server-Benutzer **59**
- Erstellen eines vCenter Server-Benutzers **56**
- Hardwareanforderungen **16**
- Hinzufügen einer View Transfer Server-Instanz **75, 76**

Lokaler Desktop, Konfiguration, Hinzufügen einer View Transfer Server-Instanz **77**

M

Mac OS X, Installieren von View Client **104**

Mediendateiformate, unterstützte **21**

Microsoft IIS-SSL-Serverzertifikate, Verwenden vorhandener Zertifikate **86**

Microsoft Windows Installer
- Befehlszeilenoptionen für die unbeaufsichtigte Installation **54**
- Eigenschaften für replizierte Instanz von View Connection Server **49**
- Eigenschaften für Sicherheitsserver **53**
- Eigenschaften für View Client **110**
- Eigenschaften für View Connection Server **45**
- MSI-Eigenschaften für View Transfer Server **83**
- View-Komponenten unbeaufsichtigt deinstallieren **55**

MMR (Multimedia Redirection) **21**

O

ODBC
- Verbindungsherstellung mit Oracle 11g oder 10g **35**
- Verbindungsherstellung mit Oracle 9i **37**
- Verbindungsherstellung mit SQL Server **33**

openssl, Dienstprogramm
- Hinzufügen zum Systempfad **86**
- Konfigurieren eines Zertifikats für View Transfer Server **92**

Oracle 10g-Datenbank
- Hinzufügen einer ODBC-Datenquelle **35**
- Hinzufügen für View Composer **34**

Oracle 11g-Datenbank
- Hinzufügen einer ODBC-Datenquelle **35**
- Hinzufügen für View Composer **34**

Oracle 9i-Datenbank
- Hinzufügen einer ODBC-Datenquelle **37**
- Hinzufügen für View Composer **36**

Organisationseinheiten, *siehe* OUs

OS X, Installieren von View Client **104**

OUs
- Erstellung für Clientkonten im Kiosk-Modus **24**
- Erstellung für View-Desktops **24**

P

PCoIP, Hardwareanforderungen **19**

PKCS#12-Format, Zertifikate **90**

PKCS#7-Format, Zertifikate **90**

Professional Services **5**

R

RDP **20**

Remote-Anzeigeprotokolle
- HP RGS **21**
- PCoIP **19**
- RDP **20**

Replizierte Instanzen
- Installieren **46**
- Netzwerkanforderungen **9**
- unbeaufsichtigte Installation **47**
- unbeaufsichtigte Installation, Eigenschaften **49**

RGS **21**

Richtlinien
- Eingeschränkte Gruppen **26**
- Vertrauenswürdige Stammzertifizierungsstellen **28**

S

Schlüsselbund **105**

Sicherheitsserver
- Ändern einer externen URL **66**
- Größenberechnung der TCB-Hash-Tabelle **70**

Installationsdatei **50**
Konfigurieren einer externen URL **65**
Konfigurieren eines Kennworts für die Paarbildung **49**
Konfigurieren zur Verwendung eines Zertifikats **91**
unbeaufsichtigte Installation **52**
unbeaufsichtigte Installation, Eigenschaften **53**
Smartcard-Authentifizierung
Active Directory-Vorbereitung **27**
Anforderungen **22**
Benutzerprinzipalnamen (UPNs) für Smartcard-Benutzer **27**
Softwareanforderungen, Serverkomponenten **7**
SQL Server Management Studio Express, installieren **32**
SQL Server-Datenbank
Hinzufügen einer ODBC-Datenquelle **33**
Hinzufügen für View Composer **32**
Vorbereiten für Ereignisdatenbank **96**
SSL
Konfigurieren für Clientverbindungen **93**
Konfigurieren für die View Transfer Server-Kommunikation **93**
SSL-Zertifikate, *siehe* Zertifikate
Stammzertifikate
Hinzufügen zu vertrauenswürdigen Stammzertifizierungsstellen **28**
Hinzufügen zum Enterprise NTAuth-Speicher **29**
Standardzertifikat, ersetzen **85**
Streaming von Multimedia **21**
Support, Online- und Telefonsupport **5**
Sysprep, Anforderungen für View Composer **11**
Systemauslagerungsdatei, Größe, Windows Server **73**

T

TCB-Hash-Tabelle
Vergrößerung auf einem Windows Server-Computer **70**
Vergrößerung für Nicht-Sicherheitsserver **69**
Vergrößerung für Sicherheitsserver **70**
Verwendung durch View **69**
TCP-Ports
View Connection Server **45**
View Transfer Server **80**
Technischer Support und Schulung **5**
ThinPrint-Einrichtung **107**
Transfer Server-Repository, konfigurieren **78**
Transmission Control Block (TCB)
Vergrößerung für Nicht-Sicherheitsserver **69**
Vergrößerung für Sicherheitsserver **70**
Verwendung durch View **69**

U

Unbeaufsichtigte Installation
Gruppenrichtlinien zum Zulassen der Installation **80, 108**
Replizierte Instanzen **47**
Sicherheitsserver **52**
View Client **108, 109**
View Client with Local Mode **109**
View Connection Server **43**
View Transfer Server **80, 81**
UPNs
Smartcard-Benutzer **27**
View Client **101**
View Client auf Mac OS X **105**
View Client with Local Mode **101**
USB-Drucker **108**
userPrincipalName, Attribut **27**

V

vCenter Server
Benutzerkonten **25, 56**
Erstellen eines Benutzers für den lokalen Modus **56**
Hinzufügen von Instanzen zu View Manager **62**
Installieren des View Composer-Dienstes **38**
Konfigurieren für View Composer **39**
vCenter Server-Benutzer
Berechtigungen für den lokalen Modus **59**
vCenter Server-Berechtigungen **58**
View Composer-Berechtigungen **59**
Vertrauensbeziehungen, konfigurieren, für View Connection Server **23**
Vertrauenswürdige Stammzertifizierungsstellen, Richtlinie **28**
View Administrator
Anforderungen **9**
Anmeldung **60**
Übersicht **60**
View Agent, Installationsanforderungen **15**
View Client
Installation auf einem Windows-PC oder -Laptop **99**
Installation über View Portal **103**
Installationsübersicht **99**
Installieren unter Mac OS X **104**
starten **99, 101, 105**
Unbeaufsichtigte Installation auf einem Windows-PC oder -Laptop **108, 109**
unbeaufsichtigte Installation, Eigenschaften **110**
unterstützte Betriebssysteme **16**

View Client with Local Mode
Gruppenrichtlinien für die unbeaufsichtigte Installation **108**
unterstützte Betriebssysteme **16**
View Client-Instanzen, Konfigurieren von Verbindungen **64**
View Composer-Datenbank
Anforderungen **31**
ODBC-Datenquelle für Oracle 11g oder 10g **35**
ODBC-Datenquelle für Oracle 9i **37**
ODBC-Datenquelle für SQL Server **33**
Oracle 11g und 10g **34**
Oracle 9i **36**
SQL Server **32**
View Composer-Infrastruktur
Konfigurieren von vSphere **39**
optimieren **39**
Testen der DNS-Auflösung **40**
View Composer-Installation
Anforderungen, Übersicht **9**
Betriebssystemanforderungen **10**
Datenbankanforderungen **10**
Installationsdatei **38**
Übersicht **31**
Virtualisierungssoftware, Anforderungen **11**
View Composer-Konfiguration
Berechtigungen für vCenter Server-Benutzer **59**
Einstellungen in View Administrator **63**
Erstellen eines Benutzerkontos **25**
Erstellen eines vCenter Server-Benutzers **25, 56**
View Connection Server-Installation
Anforderungen, Übersicht **7**
Einzelserver **42**
Hardwareanforderungen **8**
Installationsarten **41**
Netzwerkkonfiguration **9**
Produktlizenzschlüssel **61**
Replizierte Instanzen **46**
Sicherheitsserver **50**
Übersicht **41**
unbeaufsichtigt **43**
unbeaufsichtigte Installation, Eigenschaften **45**
unterstützte Betriebssysteme **8**
Virtualisierungssoftware, Anforderungen **8**
Voraussetzungen **41**
View Connection Server-Konfiguration
anfängliche **60**
Clientverbindungen **64**
Ereignisdatenbank **95, 97**
Ersetzen des Standardzertifikats **85**
externe URL **66**
Externe URL **65**
Größeneinstellungen für Windows Server **67**
Serverzertifikat **91**
Systemauslagerungsdatei, Größe **73**
Übersicht **41**
Vertrauensbeziehungen **23**
View Portal, Browseranforderungen **18**
View Secure Gateway Server-Komponente, Vergrößern des JVM-Heaps **72**
View Transfer Server-Installation
Anforderungen für virtuelle Maschinen **12**
Anforderungen, Übersicht **12**
Gruppenrichtlinien für die unbeaufsichtigte Installation **80**
Installationsdatei **76**
Speicheranforderungen **13**
Übersicht **75**
unbeaufsichtigt **80, 81**
unbeaufsichtigte Installation, Eigenschaften **83**
unterstützte Betriebssysteme **13**
View Transfer Server-Konfiguration
Hinzufügen einer Instanz **77**
Transfer Server-Repository **78**
View-Desktops, Konfigurieren direkter Verbindungen **65**
View-Komponenten, Befehlszeilenoptionen für die unbeaufsichtigte Installation **54**
Virtuelle Druckfunktion **107**
vSphere, Konfigurieren für View Composer **39**

W

Webbrowseranforderungen **9, 18**
Windows 7-Anforderungen, Desktops im lokalen Modus **16**
Windows Server, Systemauslagerungsdatei, Größe **73**
Windows-Computer, Installieren von View Client **99**
Wyse MMR **21**

Z

Zertifikate
Anforderungen **85**
Ersetzen des Standardzertifikats **85**
Erstellen neuer Zertifikate **87**
Erwerben von Signaturen **89**
Import in eine Schlüsselspeicherdatei **90**
Konfigurieren zur Verwendung durch View Connection Server **91**
Konfigurieren zur Verwendung durch View Transfer Server **92**
Konvertieren in das PKCS#7-Format **90**

Überprüfung in View Client **94**
Verwendung des keytool-Dienstprogramms zum Generieren **88**